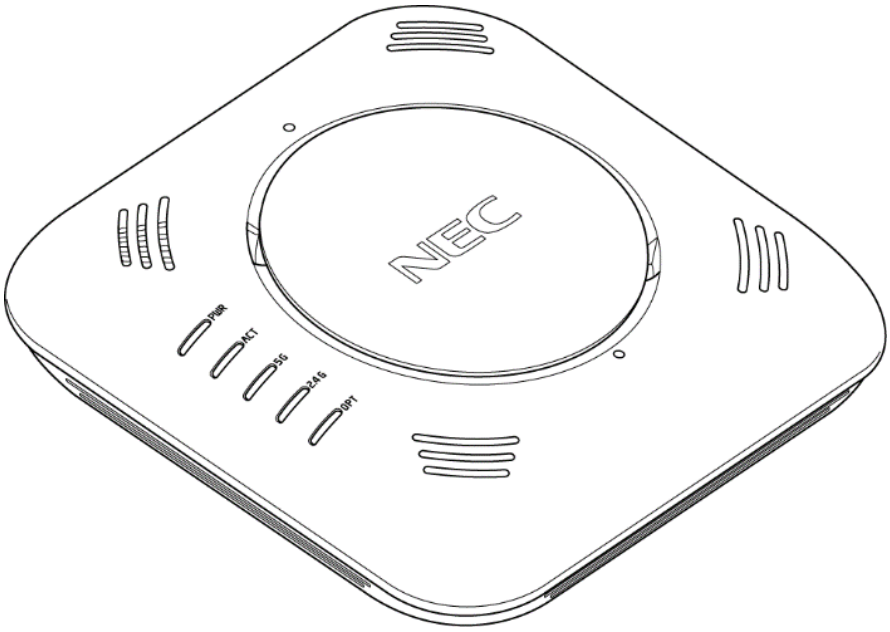
IEEE802.11ac 対応無線 LAN アクセスポイント

NA1500A



設定事例集

第 9.0 版

ご注意

本装置をご使用の前に、本書をよくお読みください。

お読みになったあとは、いつでもご覧になれる場所に必ず保管してください。

＜はじめに＞

このたびは IEEE802.11ac 対応無線 LAN アクセスポイント NA1500A をご利用いただき、まことにありがとうございます。

本書では、本装置に搭載されている各機能の詳細について説明します。

各コマンドの詳細については、「コマンドリファレンスガイド」を参照してください。
なお、本書は NA1500A ソフトウェアバージョン 9.1 に対応しています。

【ご注意】

(1) 本書の内容の一部または全部を無断転載･無断複写することは禁止されています。
(2) 本書の内容については、将来予告なしに変更することがあります。
(3) 本書の内容については万全を期して作成いたしましたが、万一ご不審な点や誤り･記載もれなどお気づきの点がありましたらご連絡ください。
(4) 本装置の故障・誤動作・天災・不具合あるいは停電などの外部要因によって通信などの機会を逸したために生じた損害などの純粋経済損失につきましては、当社は一切その責任を負いかねますのであらかじめご了承ください。
(5) セキュリティ対策をほどこさず、あるいは、無線 LAN の仕様上やむをえない事情によりセキュリティの問題が発生してしまった場合、当社は、これによって生じた損害に対する責任は一切負いかねますのであらかじめご了承ください。
(6) せっかくの機能も不適切な扱いや不測の事態（例えば落雷や漏電など）により故障してしまっては能力を発揮できません。「取扱説明書」をよくお読みになり、記載されている注意事項を必ずお守りください。

＜目次＞

＜はじめに＞ i

＜目次＞ ii

第1章　コンフィグレーションモード 1-1

1.1.　インタフェースとコンフィグレーションモードについて 1-2
1.2.　モード遷移 1-3

第2章　ログイン 2-1

2.1.　管理者アカウントで利用する 2-2
2.2.　ビューアユーザアカウントで利用する 2-3
2.3.　グローバルコンフィグレーションモードに遷移する 2-4

第3章　共通設定 3-1

3.1.　システム設定（装置共通の設定） 3-2
3.1.1.　ターミナルの表示長さの制限を変更する 3-2
3.1.2.　ターミナルのログインタイムアウト値を変更する 3-2
3.1.3.　バージョンを確認する 3-3
3.1.4.　日時を設定する 3-3
3.1.5.　ホスト名を設定する 3-3
3.1.6.　管理者アカウントのユーザ名とパスワードを変更する 3-4
3.2.　ビューアユーザを登録する 3-5

第4章　設定事例 4-1

4.1.　設定事例 1　LAN1/PoE ポートと LAN2 ポートの利用 4-2
4.1.1.　VLAN を作成する 4-3
4.1.2.　LAN1/PoE ポートと LAN2 ポートを設定する 4-12
4.2.　設定事例 2　無線インタフェースの利用 4-15
4.2.1.　無線インタフェースを設定する 4-16
4.2.2.　SSID を設定する 4-18
4.2.3.　無線インタフェースを有効設定する 4-21
4.2.4.　ステルス機能を使用する 4-22

4.2.5. レーダ波検出時のチャネル遷移を無効にする 4-23
4.2.6. チャネル自動更新スケジュールを設定する 4-25
4.2.7. 送信電力自動調整スケジュールを設定する 4-27
4.3. 設定事例 3 無線クライアントの帰属管理 4-30
4.3.1. MAC アクセスリストを登録／削除する 4-31
4.3.2. MAC アクセスリストを適用する 4-33
4.3.3. MAC アクセスリストの適用状態を確認する 4-36
4.4. 設定事例 4 RADIUS サーバ認証の設定 4-37
4.4.1. 使用するプライマリ RADIUS サーバを設定する 4-38
4.4.2. 使用するセカンダリ RADIUS サーバを設定する 4-40
4.4.3. RADIUS サーバへのアクセスブロックを設定する 4-41
4.4.4. RADIUS サーバへの再認証間隔を設定する 4-42
4.5. 設定事例 5 送信ビームフォーミングの設定 4-43
4.5.1. SU-MIMO を設定する 4-44
4.5.2. MU-MIMO を設定する 4-45
4.6. 設定事例 6 リンクインテグリティの設定 4-46
4.6.1. イーサネットインタフェースのリンク監視を設定する 4-48
4.6.2. 通信監視ホストのアドレスと監視条件を設定する 4-49
4.6.3. 無線インタフェースの停止条件を設定する 4-50
4.7. 設定事例 7 トラフィックシェーピングの設定 4-51
4.8. 設定事例 8 送信 AMPDU の設定 4-53
4.9. 設定事例 9 IP フィルタリングの設定 4-54
4.9.1. 特定の有線クライアント以外からの CLI へのアクセスを遮断する 4-54
4.9.2. 無線クライアントから本装置への Ping を許可する 4-56
4.9.3. 無線クライアントと有線クライアント間のみ通信を許可する 4-58
4.9.4. 無線クライアントからルータを経由した通信のみを許可する 4-60
4.10. 設定事例 10 NetMeister クライアントの設定 4-62
4.10.1. NetMeister クライアント設定を手動で実施 4-62
4.10.2. NetMeister クライアント設定をゼロタッチプロビジョニングで実施 4-64
4.10.3. NGN-VPN セキュアアクセスサービスの IPv6 閉域網の利用 4-66
4.11. 設定事例 11 集中管理クライアントの設定 4-71
4.12. 設定事例 12 SSID 停止スケジュールの設定 4-72
4.13. 設定事例 13 バンドステアリング（ロードバランス）の設定 4-73
4.13.1. Pre-association steering 機能 4-74
4.13.2. Idle post-association steering 機能 4-76
4.13.3. Active post-association steering 機能 4-78

4.14. 設定事例 14 ProxyARP の設定 4-80
4.14.1. ProxyARP 機能が有効（ip-proxy-arp enable [MODE]）の場合 4-80
4.14.2. ProxyARP 機能が無効（no ip-proxy-arp enable）の場合 4-81
第5章 利用シーンごとの設定例 5-1
5.1. 公共エリアでの設定利用例 5-2
5.1.1. VLAN 内の異なる SSID へ帰属した無線クライアント間通信遮断 5-3
5.1.2. 同一 SSID へ帰属した無線クライアント間通信遮断 5-4
5.1.3. 複数の NA1500A を使用した場合の無線クライアント間通信遮断 5-5
第6章 付録 6-1
商標、ライセンス、コピーライト 6-2

第１章　　コンフィグレーションモード

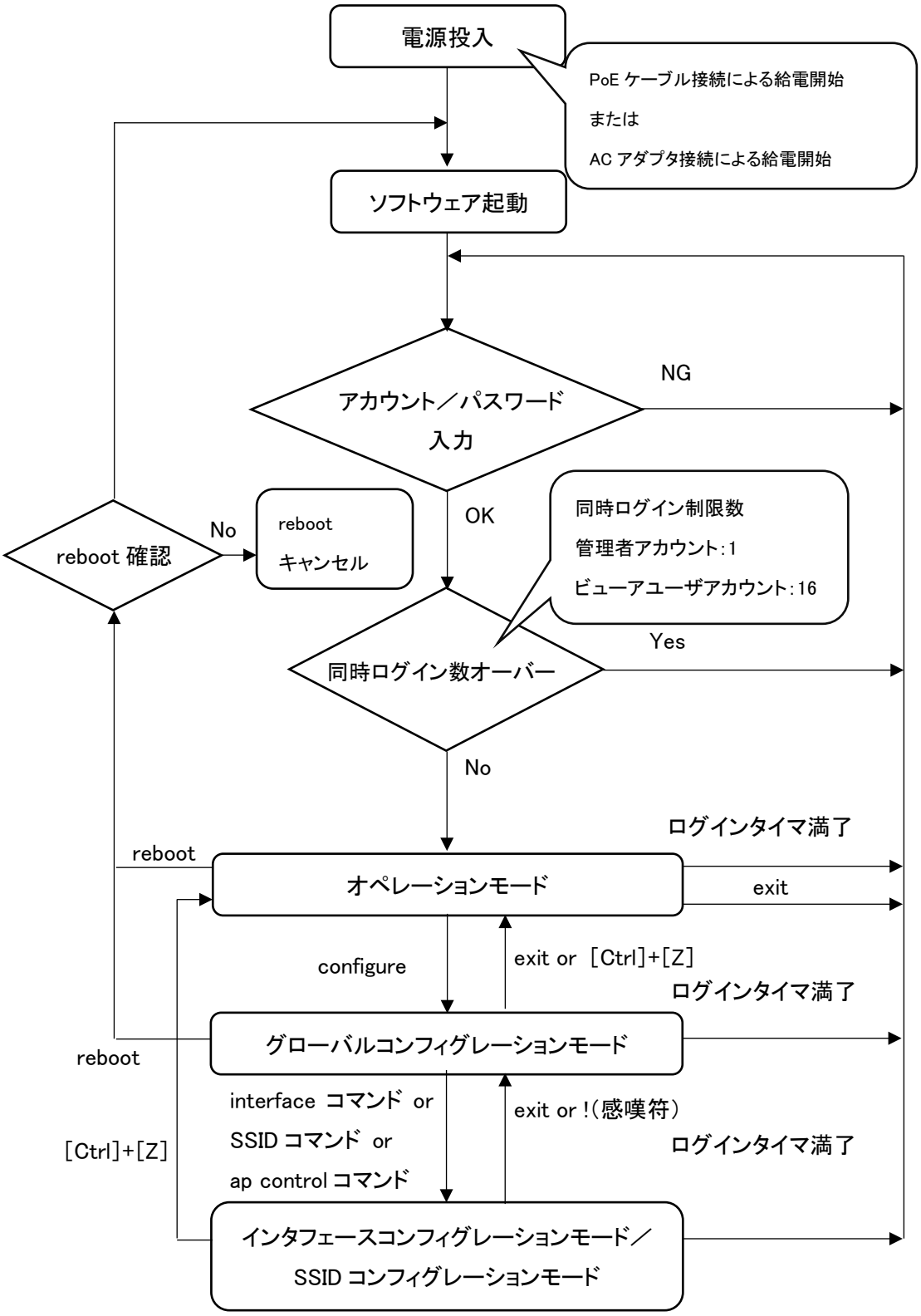
本章は、各インタフェースの設定とコンフィグレーションモードの関係について説明します。

1.1. インタフェースとコンフィグレーションモードについて

本書は、ネットワーク構成図と設定例をもとに記述しています。
ご利用いただけるインタフェース名ならびに対応するコンフィグレーションモード名は、
以下となります。

物理／論理インタフェース名称	コンフィグレーションモード名
VLAN インタフェース （論理インタフェース）	VLAN インタフェースコンフィグレーションモード
LAN1/PoE ポート （物理／基本インタフェース）	GigaEthernet0 インタフェースコンフィグレーションモード
LAN1/PoE ポート （仮想インタフェース）	GigaEthernet0.<Virtual Interface ID> インタフェースコンフィグレーションモード Virtual Interface ID は、1～16 で、最大 16 個まで使用可能
LAN2 ポート （物理／基本インタフェース）	GigaEthernet1 インタフェースコンフィグレーションモード
LAN2 ポート （仮想インタフェース）	GigaEthernet1.<Virtual Interface ID> インタフェースコンフィグレーションモード Virtual Interface ID は、1～16 で、最大 16 個まで使用可能
5GHz 帯無線インタフェース	radio0 インタフェースコンフィグレーションモード
2.4GHz 帯無線インタフェース	radio1 インタフェースコンフィグレーションモード
SSID	SSID コンフィグレーションモード

1.2. モード遷移


電源投入
PoE ケーブル接続による給電開始
または
AC アダプタ接続による給電開始
ソフトウェア起動
アカウント／パスワード
入力
NG
OK
同時ログイン制限数
管理者アカウント：1
ビューアユーザアカウント：16
reboot 確認
No
reboot
キャンセル
同時ログイン数オーバー
Yes
No
ログインタイマ満了
reboot
オペレーションモード
exit
configure
exit or ［Ctrl］+[Z]
ログインタイマ満了
グローバルコンフィグレーションモード
reboot
interface コマンド or
SSID コマンド or
ap control コマンド
exit or !（感嘆符）
ログインタイマ満了
[Ctrl]+[Z]
インタフェースコンフィグレーションモード／
SSID コンフィグレーションモード

第2章　　ログイン

本章は、ログイン方法について説明します。

2.1. 管理者アカウントで利用する

管理者アカウントで使用する場合、初回ログイン時

login config

Password config

初回ログインするとユーザ名とパスワードの変更を求められます。

管理者アカウント ユーザ名（New username）で使用できる文字

アスキー文字列。大文字／小文字は区別されます。

範囲: 8～16 文字

使用できる文字

アルファベット半角大文字（A～Z）

アルファベット半角小文字（a～z）

数字半角（0～9）

記号半角「-（ハイフン）」、「_（アンダースコア）」

※ただし、先頭に「-（ハイフン）」は使用できません。

管理者アカウント パスワード（New password）で使用できる文字

アスキー文字列。大文字／小文字は区別されます。

範囲: 8～249 文字

使用できる文字

アルファベット半角大文字（A～Z）

アルファベット半角小文字（a～z）

数字半角（0～9）

記号半角

（下記は、わかりやすくするために全角で表示しています。）

！	“	＃	＄	％	＆	（	）
＊	＋	,	－	.	／	：	；
＜	＝	＞	＠	［	＼	］	＾
＿	｛	｜	｝	～			

【注意】パスワードは、推測困難な文字列の組み合わせにて設定してください。

変更後、「write memory」を必ず行ってください。

ログインすると以下のプロンプトが表示され、オペレーションモードが表示されます。

AP#

2.2. ビューアユーザアカウントで利用する

登録済みビューアユーザのアカウント／パスワードで、ログインします。

例

login: Taro_XXXX　　登録済みビューアユーザアカウント

Password: XXXXXXXXXX　　登録済みビューアユーザパスワード

ログインすると以下のプロンプトが表示され、オペレーションモードが表示されます。

AP#

ビューアユーザのアカウントで使用できるコマンド一覧

オペレーションモード	グローバルコンフィグレーションモード
configure exit show copyright	exit ?（help 相当） show arp entry show arp statistics show associations show buffers show clock show copyright show error-log show hardware show interfaces show ip filter show led show logging show mac filter show memory show ntp show power inline show processes show radio-nol show rogue ap show snmp-agent community show ssh-server sessions show terminal show uptime show version

2.3. グローバルコンフィグレーションモードに遷移する

以下コマンドにて、グローバルコンフィグレーションモードに移行ができます。

```
AP# configure
Enter configuration commands, one per line. End with CTRL+Z.
AP(config)#
```

上記のとおり、プロンプトが変化します。

第3章　　共通設定

本章は、システムの共通設定について説明します。

3.1. システム設定（装置共通の設定）

3.1.1. ターミナルの表示長さの制限を変更する

以下コマンドにて、ターミナルの表示長さ制限を変更できます。

100 行に制限する場合

AP(config)# terminal length 100

※設定変更後の動作は即時反映です。

ソフトウェアバージョン 4.0 以降は、本設定値は保存されず、

再起動すると初期値に戻ります。

初期値に関しては、「コマンドリファレンスガイド」を参照してください。

長さ制限を行わない場合

AP(config)# terminal length 0

※設定変更後の動作は即時反映です。

ソフトウェアバージョン 4.0 以降は、本設定値は保存されず、

再起動すると初期値に戻ります。

初期値に関しては、「コマンドリファレンスガイド」を参照してください。

3.1.2. ターミナルのログインタイムアウト値を変更する

以下コマンドにて、ターミナルのログインタイムアウト値を変更できます。

タイムアウト時間を 10 分に設定する場合

AP(config)# terminal timeout 10

※設定変更後の動作は即時反映です。

ソフトウェアバージョン 4.0 以降は、本設定値は保存されず、

再起動すると初期値に戻ります。

初期値に関しては、「コマンドリファレンスガイド」を参照してください。

タイムアウトしないようにする場合

AP(config)# terminal timeout 0

※設定変更後の動作は即時反映です。

ソフトウェアバージョン 4.0 以降は、本設定値は保存されず、

再起動すると初期値に戻ります。

初期値に関しては、「コマンドリファレンスガイド」を参照してください。

3.1.3. バージョンを確認する

以下コマンドにて、バージョンの確認ができます。

```
AP(config)# show ver
Boot ver.       : Boot Version X.X.X
FW
   Boot side            : normal
   FW ver.              : Y.Y.Y
   FW ver.(backup)   : Z.Z.Z
```

3.1.4. 日時を設定する

以下コマンドにて、日時の設定ができます。

```
AP(config)# clock 17 20 0 31 5 2018
% Thu May 31 17:20:00 JST 2018
```

日時設定項目は、以下のとおりです。

clock HOUR MINUTE SECONDS [DATE [MONTH [YEAR]]]

3.1.5. ホスト名を設定する

以下コマンドにて、ホスト名表示を変更できます。

```
AP(config)# hostname na1500a
AP(config)# write memory
```

3.1.6. 管理者アカウントのユーザ名とパスワードを変更する

以下のコマンドにて、管理者アカウントのユーザ名とパスワードを変更できます。

admin-name USER-NAME password { plain Plain-PW | secret Secret-PW }

平文のパスワードを使用して設定する場合の例
AP(config)# admin-name ABCD-EFGH password plain Plain-PW

暗号化されたパスワードを使用して設定する場合の例
AP(config)# admin-name ABCD-EFGH password secret XXXXXXXXXXXXXX

設定後は、必ず「write memory」コマンドを使用して保存してください。
AP(config)# write memory

【注意】
本コマンドを使用することで、変更後の管理者アカウントのユーザ名と
暗号化されたパスワードを「show running-config」にて確認することが
できるようになります。
本コマンド未使用時は、「show running-config」で表示されません。
本コマンドを使用することで、管理者アカウントは上書きされ、旧管理者アカウントは
使用できなくなります。
本コマンドを使用して変更したあと、CLI および設定ツールなどからのログインは、
変更後のユーザ名とパスワードを使用してください。

3.2. ビューアユーザを登録する

ビューアユーザアカウントは、1 つだけ作成できます。
以下のビューアユーザ名／ビューアユーザパスワードを登録したい場合、
次の設定を行います。

例　ユーザ名:　Taro_XXXX
　　パスワード:　Taro_XXXX_abcd_12345678

```
AP(config)# username Taro_XXXX Taro_XXXX_abcd_12345678
AP(config)# write memory
```

登録に使用できる文字は、以下のとおりです。

ユーザ名

アスキー文字列。大文字／小文字は区別されます。

範囲: 8～16 文字

使用できる文字

アルファベット半角大文字（A～Z）

アルファベット半角小文字（a～z）

数字半角（0～9）

記号半角「-（ハイフン）」、「_（アンダースコア）」

※ただし、先頭に「-（ハイフン）」は使用できません。

パスワード

アスキー文字列。大文字／小文字は区別されます。

範囲: 8～249 文字

使用できる文字

アルファベット半角大文字（A～Z）

アルファベット半角小文字（a～z）

数字半角（0～9）

記号半角

（下記は、わかりやすくするために全角で表示しています。）

!	“	#	$	%	&	(	)
*	+	,	−	.	／	:	;
<	=	>	@	[	＼	]	^
_	{	|	}	～			

【注意】パスワードは、推測困難な文字列の組み合わせにて設定してください。

第4章　　設定事例

各種機能の設定について説明します。

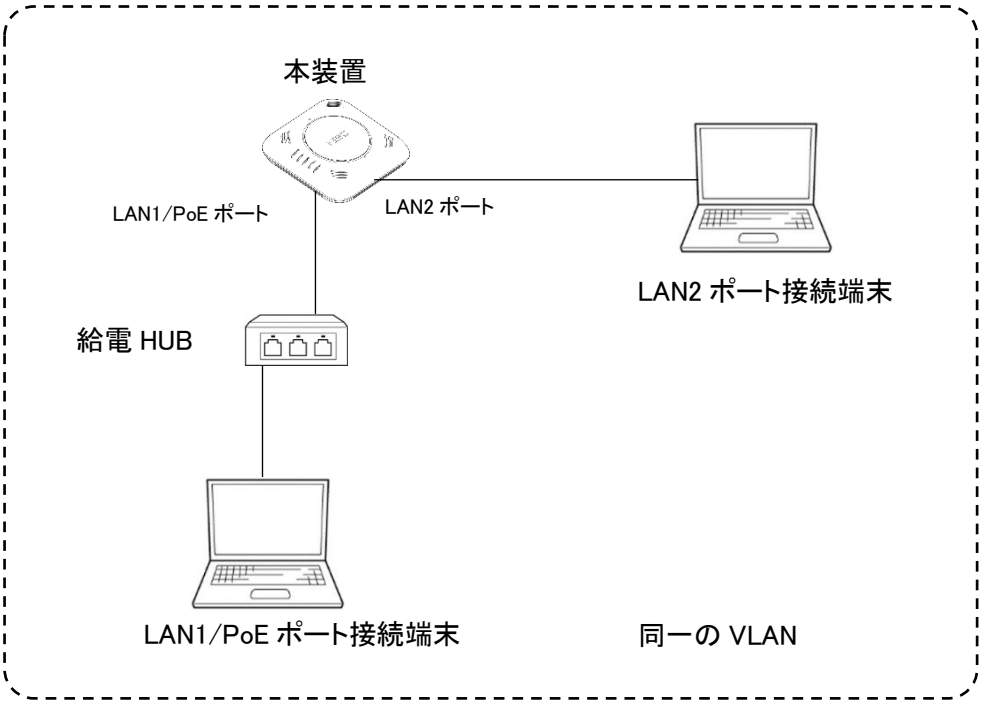
4.1. 設定事例 1 LAN1/PoE ポートと LAN2 ポートの利用

1 つの VLAN 内に

LAN1/PoE ポート

LAN2 ポート

の構成を登録して利用する場合の事例です。



4.1.1. VLAN を作成する

以下のコマンドにて、設定可能 VLAN-ID を確認できます。

```
AP(config)# interface vlan ?
  <1-4094>  -- config_interface_vlan
  u         -- config_interface_vlan
```

ソフトウェアバージョンにより同時に使用できる VLAN の組み合わせが異なります。

ソフトウェアバージョン 1.0 は、Untagged-VLAN（VLAN-ID は、u）または、
Tagged-VLAN（VLAN-ID は、1～4094）のいずれかしか設定できません。
そのため、複数の VLAN を同時に使用したい場合は、Tagged-VLAN を使用します。
（Tagged パケットによる使用）

ソフトウェアバージョン 2.0 以降は、Untagged-VLAN（VLAN-ID は、u）と
Tagged-VLAN（VLAN-ID は、1～4094）を、同時に使用できます。

いずれのソフトウェアバージョンでも Untagged-VLAN は、1 つまでしか使用できません。

4.1.1.1. Untagged-VLAN を設定する

使用する装置の IPv4 アドレスおよび IPv6 アドレスを

・IPv4 アドレスを固定設定する場合

・IPv4 アドレスの DHCP による自動割り当てを使用する場合

・IPv6 アドレスのルータからの RA 通知による自動設定を使用する場合

・IPv4 アドレスおよび IPv6 アドレスを割り当てない

のいずれかにより、次の設定を行ってください。

IPv4 アドレスおよび IPv6 アドレスは、複数の VLAN を使用する場合、

いずれかの VLAN にて、1 つまで設定が可能です。

（1）　IPv4 アドレスを固定設定する

以下は、IPv4 アドレスを固定で使用する場合の例です。

```
AP(config)# interface vlan u
AP(config-vlan u)# ip address 192.168.1.245/24
AP(config-vlan u)# ip route 192.168.1.1
AP(config-vlan u)# dns server 192.168.1.1
AP(config-vlan u)# vlan enable
AP(config-vlan u)# !
AP(config)# write memory
```

（2）　IPv4 アドレスの DHCP による自動割り当てを使用する

以下は、IPv4 アドレス、IPv4 ゲートウェイアドレス、IPv4DNS サーバアドレスの DHCP による自動割り当てを使用する場合の例です。

```
AP(config)# interface vlan u
AP(config-vlan u)# ip address dhcp
AP(config-vlan u)# dns server dhcp
AP(config-vlan u)# vlan enable
AP(config-vlan u)# !
AP(config)# write memory
```

IPv4DNS サーバは、複数設定が可能です。
使用しない IPv4DNS サーバは、以下のコマンドで削除が可能です。
以下は、登録済み IPv4DNS サーバ（192.168.1.1）を削除する場合の例です。

```
AP(config)# interface vlan u
AP(config-vlan u)# no dns server 192.168.1.1
AP(config-vlan u)# !
AP(config)# write memory
```

（3）　IPv6 アドレスのルータからの RA 通知による自動設定を使用する

以下は、IPv6 アドレス、IPv6 ゲートウェイアドレス、IPv6DNS サーバアドレスのルータからの
RA 通知による自動設定を使用する場合の例です。
※「ipv6 enable」は、IPv4 アドレスが固定設定されるか、または DHCP による自動割り当てに
　設定されているマネージメント VLAN のみ設定が可能です。

IPv4 アドレスが、固定設定の場合

```
AP(config)# interface vlan u
AP(config-vlan u)# ip address 192.168.1.245/24
AP(config-vlan u)# ip route 192.168.1.1
AP(config-vlan u)# dns server 192.168.1.1
AP(config-vlan u)# ipv6 enable
AP(config-vlan u)# !
AP(config)# write memory
```

IPv4 アドレスが、DHCP による自動割り当てに設定されている場合

```
AP(config)# interface vlan u
AP(config-vlan u)# ip address dhcp
AP(config-vlan u)# dns server dhcp
AP(config-vlan u)# ipv6 enable
AP(config-vlan u)# !
AP(config)# write memory
```

本設定の場合、以下のアドレスが、自動生成ならびに設定が行われます。

IPv6 アドレス
　　RA から本装置の IPv6 アドレスを生成します。

IPv6 ゲートウェイ
　　RA を通知するパケットの送信元アドレスを IPv6 用の
　　デフォルトゲートウェイアドレスとします。

IPv6DNS サーバ
　　RA を通知するパケットの送信元アドレスを IPv6 用の
　　DNS サーバアドレスとします。

IPv6 アドレスを使用しない場合は、以下のコマンドで削除が可能です。

```
AP(config)# interface vlan u
AP(config-vlan u)# no ipv6 enable
AP(config-vlan u)# !
AP(config)# write memory
```

4.1.1.2. Tagged-VLAN（例 VLAN-ID=2）を設定する

使用する装置の IPv4 アドレスおよび IPv6 アドレスを

・IPv4 アドレスを固定設定する場合

・IPv4 アドレスの DHCP による自動割り当てを使用する場合

・IPv6 アドレスのルータからの RA 通知による自動設定を使用する場合

・IPv4 アドレスおよび IPv6 アドレスを割り当てない

のいずれかにより、次の設定を行ってください。

IPv4 アドレスおよび IPv6 アドレスは、複数の VLAN を使用する場合、

いずれかの VLAN にて、1 つまで設定が可能です。

（1）　IPv4 アドレスを固定設定する

以下のコマンドにて、VLAN に固定アドレスを設定することができます。

```
AP(config)# interface vlan 2  ・・・・・・・・VLAN-ID=2 を指定
AP(config-vlan 2)# ip address 192.168.1.245/24
AP(config-vlan 2)# ip route 192.168.1.1
AP(config-vlan 2)# dns server 192.168.1.1
AP(config-vlan 2)# vlan enable
AP(config-vlan 2)# !
AP(config)# write memory
```

（2）　IPv4 アドレスの DHCP による自動割り当てを使用する

以下は、IPv4 アドレス、IPv4 ゲートウェイアドレス、IPv4DNS サーバアドレスの DHCP による
自動割り当てを使用する場合の例です。

```
AP(config)# interface vlan 2
AP(config-vlan 2)# ip address dhcp
AP(config-vlan 2)# dns server dhcp
AP(config-vlan 2)# vlan enable
AP(config-vlan 2)# !
AP(config)# write memory
```

IPv4DNS サーバは、複数設定が可能です。
使用しない IPv4DNS サーバは、以下のコマンドで削除が可能です。
以下は、登録済み IPv4DNS サーバ（192.168.1.1）を削除する場合の例です。

```
AP(config)# interface vlan 2
AP(config-vlan 2)# no dns server 192.168.1.1
AP(config-vlan 2)# !
AP(config)# write memory
```

（3）　IPv6 アドレスのルータからの RA 通知による自動設定を使用する

以下は、IPv6 アドレス、IPv6 ゲートウェイアドレス、IPv6DNS サーバアドレスのルータからの
RA 通知による自動設定を使用する場合の例です。
※「ipv6 enable」は、IPv4 アドレスが固定設定されるか、または DHCP による自動割り当てに
　設定されているマネージメント VLAN のみ設定が可能です。

IPv4 アドレスが、固定設定の場合

```
AP(config)# interface vlan 2
AP(config-vlan 2)# ip address 192.168.1.245/24
AP(config-vlan 2)# ip route 192.168.1.1
AP(config-vlan 2)# dns server 192.168.1.1
AP(config-vlan 2)# ipv6 enable
AP(config-vlan 2)# !
AP(config)# write memory
```

IPv4 アドレスが、DHCP による自動割り当てに設定されている場合

```
AP(config)# interface vlan 2
AP(config-vlan 2)# ip address dhcp
AP(config-vlan 2)# dns server dhcp
AP(config-vlan 2)# ipv6 enable
AP(config-vlan 2)# !
AP(config)# write memory
```

本設定の場合、以下のアドレスが、自動生成ならびに設定が行われます。

IPv6 アドレス
　　RA から本装置の IPv6 アドレスを生成します。
IPv6 ゲートウェイ
　　RA を通知するパケットの送信元アドレスを IPv6 用の
　　デフォルトゲートウェイアドレスとします。
IPv6DNS サーバ
　　RA を通知するパケットの送信元アドレスを IPv6 用の
　　DNS サーバアドレスとします。

IPv6 アドレスを使用しない場合は、以下のコマンドで削除が可能です。

```
AP(config)# interface vlan 2
AP(config-vlan 2)# no ipv6 enable
AP(config-vlan 2)# !
AP(config)# write memory
```

4.1.2. LAN1/PoE ポートと LAN2 ポートを設定する

以降、LAN1/PoE ポート（GigaEthernet0）インタフェースを例に説明します。
LAN2 ポート（GigaEthernet1）を設定したい場合は、GigaEthernet0 を GigaEthernet1 に読み替えて設定します。

4.1.2.1 LAN1/PoE ポートの物理インタフェースを設定する

以下のコマンドにて、物理インタフェースの設定を行うことができます。

```
AP(config)# interface GigaEthernet0
AP(config-if-GigaEthernet0)# port-speed auto  ･･･スピード/Duplex を Auto に設定
AP(config-if-GigaEthernet0)# no port-mdi-mdix  ･･･････Mdi/Mdix を Auto に設定
AP(config-if-GigaEthernet0)# no port-shutdown  ･･･････ポートをアクティブに設定
AP(config-if-GigaEthernet0)# !
AP(config)# write memory
```

4.1.2.2 LAN1/PoE ポートの VLAN を登録する

4.1.2.2.1 LAN1/PoE ポートの VLAN を Untagged-VLAN に接続設定する

以下のコマンドにて、VLAN の設定を行うことができます。

```
AP(config)# interface GigaEthernet0
AP(config-if-GigaEthernet0)# vlan u  ・・・・・・・・・・作成済みの Untagged-VLAN の ID
AP(config-if-GigaEthernet0)# no shutdown
AP(config-if-GigaEthernet0)# !
AP(config)# write memory
```

4.1.2.2.2 LAN1/PoE ポートの VLAN を Tagged-VLAN に接続設定する

Tagged_VLAN を使用する場合は、下記、Virtual Interface ID（X）を使用します。

GigaEthernet0.X

下記では、Virtual Interface ID に「1」を使用します。

```
AP(config)# interface GigaEthernet0.1
AP(config-if-GigaEthernet0.1)# vlan 2  ・・・・・・作成済みの Tagged-VLAN の ID
AP(config-if-GigaEthernet0.1)# no shutdown
AP(config-if-GigaEthernet0.1)# !
AP(config)# write memory
```

4.1.2.3 LAN2 ポートの物理インタフェースを設定する

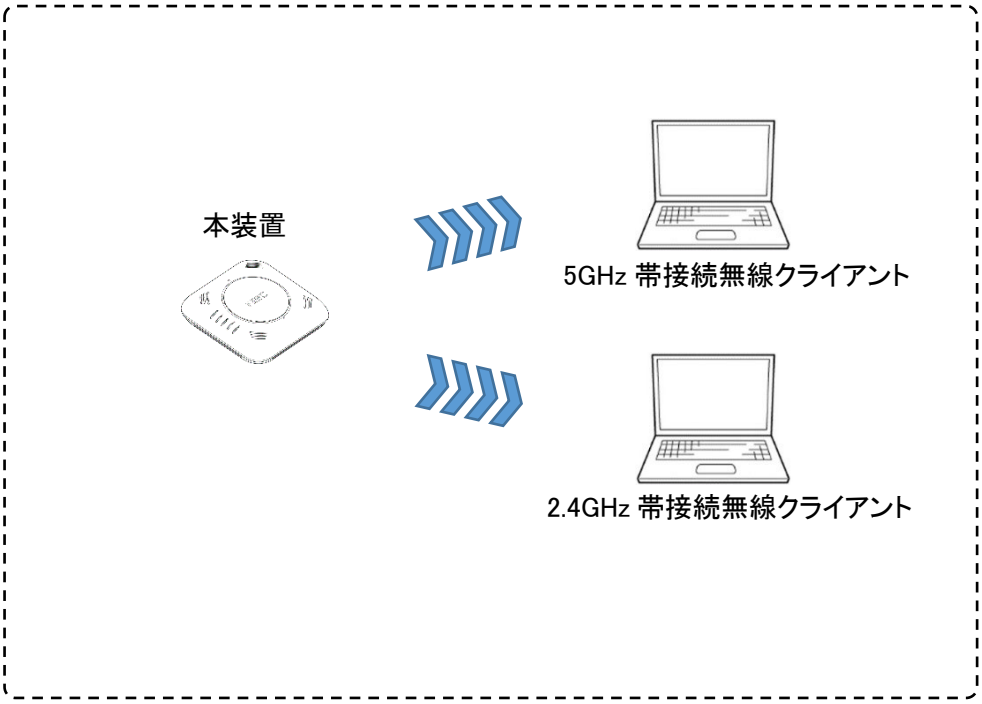
「4.1.2.1 LAN1/PoE ポートの物理インタフェースを設定する」を
LAN2 ポート（GigaEthernet1）に読み替えて設定します。

4.1.2.4 LAN2 ポートの VLAN を登録する

「4.1.2.2 LAN1/PoE ポートの VLAN を登録する」を
LAN2 ポート（GigaEthernet1）に読み替えて設定します。

4.2.　設定事例 2　無線インタフェースの利用

無線インタフェースの設定、SSID 設定についての事例です。



4.2.1. 無線インタフェースを設定する

4.2.1.1. 5GHz 帯無線インタフェース（radio0）を設定する

例 1）以下の内容を設定します。

Channel　　36 固定
通信規格（モード） 11ac を使用
バンド幅　　80MHz

```
AP(config)# interface radio0
AP(config-if-radio0)# channel 36 mode 11ac bandwidth 80
AP(config-if-radio0)# !
AP(config)# write memory
```

例 2）以下の内容を設定します。

Channel　　36 固定
通信規格（モード） 11ac を使用
バンド幅　　40MHz

```
AP(config)# interface radio0
AP(config-if-radio0)# channel 36 mode 11ac bandwidth 40
AP(config-if-radio0)# !
AP(config)# write memory
```

例 3）以下の内容を設定します。

Channel　　36 固定
通信規格（モード） 11ac を使用
バンド幅　　20MHz

```
AP(config)# interface radio0
AP(config-if-radio0)# channel 36 mode 11ac bandwidth 20
AP(config-if-radio0)# !
AP(config)# write memory
```

4.2.1.2. 2.4GHz 帯無線インタフェース（radio1）を設定する

例 1）以下の内容を設定します。

Channel　　1 固定
通信規格（モード）11ng を使用
バンド幅　　40MHz

```
AP(config)# interface radio1
AP(config-if-radio1)# channel 1 mode 11ng bandwidth 40
AP(config-if-radio1)# !
AP(config)# write memory
```

例 2）以下の内容を設定します。

Channel　　1 固定
通信規格（モード）11ng を使用
バンド幅　　20MHz

```
AP(config)# interface radio1
AP(config-if-radio1)# channel 1 mode 11ng bandwidth 20
AP(config-if-radio1)# !
AP(config)# write memory
```

4.2.2. SSID を設定する

4.2.2.1. 5GHz 帯無線インタフェース（radio0）専用 SSID を作成する

例）以下の内容を設定します。

SSID 名	test_5G
無線クライアント許容台数	10 台
認証モード	WPA2-PSK
暗号化	AES
パスフレーズ	12345678
接続先 VLAN-ID	u
使用周波数	5GHz 帯（radio0）

SSID を作成し SSID コンフィグレーションモードにて設定します。

```
AP(config)# ssid test_5G
AP(config-ssid test_5G)# max-associations 10
AP(config-ssid test_5G)# vlan u・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・VLAN-ID を指定
AP(config-ssid test_5G)# encryption mode wpa2 aes・・・・・・・・・・・・・・・・・wpa2-aes 指定
AP(config-ssid test_5G)# authentication type psk・・・・・・・・・・・・・・・・・・・・psk 指定
AP(config-ssid test_5G)# encryption wpa-psk-key ascii 12345678・・・パスフレーズ設定
AP(config-ssid test_5G)# radio-device radio0・・・・・・使用する無線インタフェースの指定
AP(config-ssid test_5G)# enable-ssid
AP(config-ssid test_5G)# !
AP(config)# write memory
```

4.2.2.2. 2.4GHz 帯無線インタフェース（radio1）専用 SSID を作成する

例）以下の内容を設定します。

SSID 名	test_2G
無線クライアント許容台数	10 台
認証モード	WPA2-PSK
暗号化	AES
パスフレーズ	12345678
接続先 VLAN-ID	u
使用周波数	2.4GHz 帯（radio1）

SSID を作成し SSID コンフィグレーションモードにて設定します。

```
AP(config)# ssid test_2G
AP(config-ssid test_2G)# max-associations 50
AP(config-ssid test_2G)# vlan u・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・VLAN-ID を指定
AP(config-ssid test_2G)# encryption mode wpa2 aes・・・・・・・・・・・・・・・・・wpa2-aes 指定
AP(config-ssid test_2G)# authentication type psk・・・・・・・・・・・・・・・・・・・・psk 指定
AP(config-ssid test_2G)# encryption wpa-psk-key ascii 12345678・・・パスフレーズ設定
AP(config-ssid test_2G)# radio-device radio1・・・・・・使用する無線インタフェースの指定
AP(config-ssid test_2G)# enable-ssid
AP(config-ssid test_2G)# !
AP(config)# write memory
```

4.2.2.3. 5GHz 帯(radio0)/2.4GHz 帯(radio1)用 SSID を作成する

例)以下の内容を設定します。

SSID 名	test_dual
無線クライアント許容台数	10 台
認証モード	WPA2-PSK
暗号化	AES
パスフレーズ	12345678
接続先 VLAN-ID	u
使用周波数	5GHz 帯および 2.4GHz 帯(both)

SSID を作成し SSID コンフィグレーションモードにて設定します。

```
AP(config)# ssid test_dual
AP(config-ssid test_dual)# max-associations 10
AP(config-ssid test_dual)# vlan u・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・VLAN-ID を指定
AP(config-ssid test_dual)# encryption mode wpa2 aes・・・・・・・・・・・・・・・wpa2-aes 指定
AP(config-ssid test_dual)# authentication type psk・・・・・・・・・・・・・・・・・psk 指定
AP(config-ssid test_dual)# encryption wpa-psk-key ascii 12345678・・パスフレーズ設定
AP(config-ssid test_dual)# radio-device both・・・・・・使用する無線インタフェースの指定
AP(config-ssid test_dual)# enable-ssid
AP(config-ssid test_dual)# !
AP(config)# write memory
```

4.2.3.　無線インタフェースを有効設定する

4.2.3.1. radio0（5GHz 帯）のみを有効にする

以下のコマンドにて、有効設定ができます。

```
AP(config)# radio-enable radio0
AP(config)# write memory
```

4.2.3.2. radio1（2.4GHz 帯）のみを有効にする

以下のコマンドにて、有効設定ができます。

```
AP(config)# radio-enable radio1
AP(config)# write memory
```

4.2.3.3. radio0（5GHz 帯）/radio1（2.4GHz 帯）とも、有効にする

以下のコマンドにて、有効設定ができます。

```
AP(config)# radio_enable both
AP(config)# write memory
```

4.2.4. ステルス機能を使用する

ステルス機能は、SSID ごとに設定を行います。

設定は、SSID コンフィグレーションモードにて、SSID 単位で行います。
以下のとおり、作成済み SSID にステルス機能を設定します。
SSID 名 :test をステルスにする場合

```
AP(config)# ssid test
AP(config-ssid test)# hide bssid
AP(config-ssid test)# !
AP(config)# write memory
```

5GHz 帯/2.4GHz 帯にて同一の SSID を使用している場合は、該当 SSID に設定すると
5GHz 帯/2.4GHz 帯両方の該当 SSID に適用されます。
ステルスを解除したい場合は、SSID コンフィグレーションモードで、以下の例のとおり
「no hide bssid」を設定します。

```
AP(config)# ssid test
AP(config-ssid test)# no hide bssid
AP(config-ssid test)# !
AP(config)# write memory
```

4.2.5. レーダ波検出時のチャネル遷移を無効にする

W53 帯または W56 帯の固定チャネル設定を使用しての動作中に限り、レーダ波を検出した際のチャネル利用について固定チャネルの継続利用を設定することができます。

dfs channel fix コマンドを使用することで、W53 帯または W56 帯の固定チャネルで動作中にレーダ波を検出したとき、他のチャネル利用をしないよう制限することができます。
本コマンドを有効にして W53 帯または W56 帯の固定チャネル使用中、レーダ波を検出すると現在使用のチャネルが、「NOL」にある間は、無線を停波します。
そして「NOL」リストから該当チャネルが消えると同一に使用していた固定チャネルにて無線復旧します。
本コマンドは、動作モードを設定する channel コマンドの内容にて、W53 帯または W56 帯の固定チャネルを設定した場合のみ有効です。

channel コマンドの設定とレーダ波検出時のチャネル遷移動作は、以下のとおりです。

<table>
<tr><td>channel コマンドで
設定した動作モード</td><td>dfs channel fix 設定時
（固定有効）
レーダ波検出時のチャネル遷移動作</td><td>no dfs channel fix 設定時
（固定無効 = 初期値）
レーダ波検出時のチャネル遷移動作</td></tr>
<tr><td>W52 帯のいずれかの
固定チャネル設定時</td><td colspan="2">W52 帯での使用中は、レーダ波を検出しません。</td></tr>
<tr><td>W53 帯のいずれかの
固定チャネル設定時</td><td rowspan="2">チャネル遷移は行わず、無線停波。
「NOL」リストから該当チャネルが消えると同一固定チャネルにて復旧します。</td><td>W53 帯のいずれかのチャネルに遷移します。</td></tr>
<tr><td>W56 帯のいずれかの
固定チャネル設定時</td><td>W56 帯のいずれかのチャネルに遷移します。</td></tr>
<tr><td>auto-w52 設定時</td><td colspan="2">W52 帯での使用中は、レーダ波を検出しません。</td></tr>
<tr><td>auto-w53 設定時</td><td colspan="2">W53 帯のいずれかのチャネルに遷移します。</td></tr>
<tr><td>auto-w56 設定時</td><td colspan="2">W56 帯のいずれかのチャネルに遷移します。</td></tr>
<tr><td>auto-w52-w53 設定時</td><td colspan="2">W53 帯にて通信時、W52/W53 帯のいずれかのチャネルに遷移します。
（W52 帯での使用中は、レーダ波を検出しません。）</td></tr>
<tr><td>auto-w52-w56 設定時</td><td colspan="2">W56 帯にて通信時、W52/W56 帯のいずれかのチャネルに遷移します。
（W52 帯での使用中は、レーダ波を検出しません。）</td></tr>
<tr><td>auto-w53-w56 設定時</td><td colspan="2">W53/W56 帯のいずれかのチャネルに遷移します。</td></tr>
<tr><td>Auto 設定時</td><td colspan="2">W52/W53/W56 帯のいずれかのチャネルに遷移します。
（W52 帯での使用中は、レーダ波を検出しません。）</td></tr>
</table>

本設定は、5GHz 帯の radio0 インタフェースコンフィグレーションモードのみ設定できます。

AP(config)# interface radio0・・・・・radio0 インタフェースコンフィグレーションモード移行
AP(config-if-radio0)# dfs channel fix・・・・固定チャネル使用有効を設定
AP(config-if-radio0)# !
AP(config)# write memory

4.2.6.　チャネル自動更新スケジュールを設定する

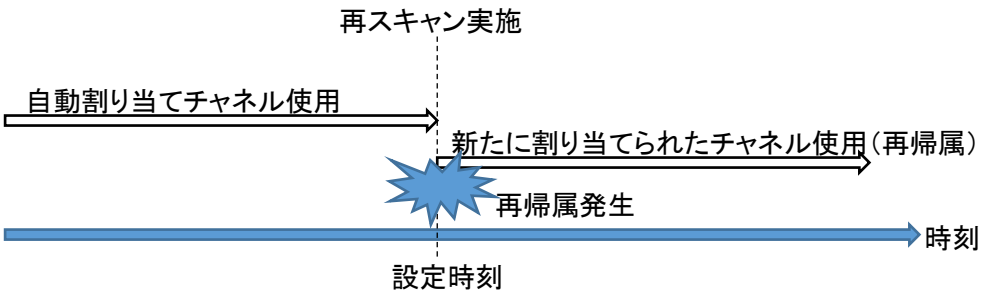
※本機能は、あらかじめ「clock」コマンド または時刻同期機能を使用して時刻設定
　する必要があります。

設定した時刻に空きチャネルを自動的に再スキャンし、チャネル自動更新をすることができます。
無線インタフェース（radio0／radio1）ごとに、最大 2 個までスケジュールを設定することができます。
ただし、スケジュール設定時刻は、送信電力自動調整スケジュールと共通になります。

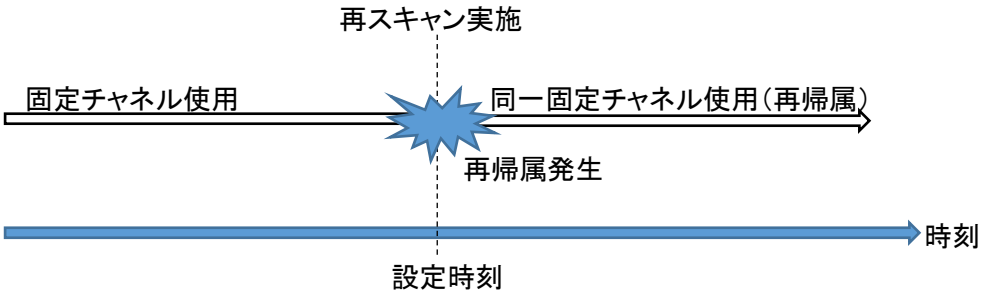
また、設定時刻の時点で、帰属無線クライアントがある場合、初期状態ではチャネル自動更新を
行わない設定ですが、チャネル自動更新を強制的に行う設定も可能です。

自動割り当てチャネル使用時、チャネル自動更新を強制的に行う設定になっている場合、
設定時刻にいったん帰属が外れ、無線クライアントの再帰属が発生します。
固定チャネル使用時、チャネル自動更新を強制的に行う設定になっている場合、
設定時刻にいったん帰属が外れますが、無線クライアントは、再度同一固定チャネルにて使用を
開始します。

チャネル自動設定の場合（channel-scan-schedule force 有効時）



固定チャネル設定の場合（channel-scan-schedule force 有効時）



動作設定例

本設定は、radio0 または radio1 のインタフェースコンフィグレーションモードにて設定が可能です。
以下は、radio0 インタフェースの設定例になります。

対象インタフェース	radio0
チャネル自動更新のスケジュール	23:30（channel-scan-schedule add TIME） ※送信電力自動調整時刻と共通
チャネル自動更新強制実施	無効（no channel-scan-schedule force）
チャネル自動更新機能	有効（channel-scan-schedule enable）

```
AP(config)# interface radio0・・・・・・・・・インタフェースコンフィグレーションモードに遷移
AP(config-if-radio0)# channel-scan-schedule add 23:30
                              ・・・・・・・・チャネル自動更新時刻 23:30 に設定
                                ※送信電力自動調整時刻と共通
AP(config-if-radio0)# no channel-scan-schedule force
                              ・・・・・・・・帰属無線クライアントがある場合、
                                チャネル自動更新を実施しない
AP(config-if-radio0)# channel-scan-schedule enable
                              ・・・・・・・・チャネル自動更新スケジュール有効
AP(config-if-radio0)# !
AP(config)# write memory
```

4.2.7. 送信電力自動調整スケジュールを設定する

※本機能は、あらかじめ「clock」コマンド または時刻同期機能を使用して時刻設定
する必要があります。

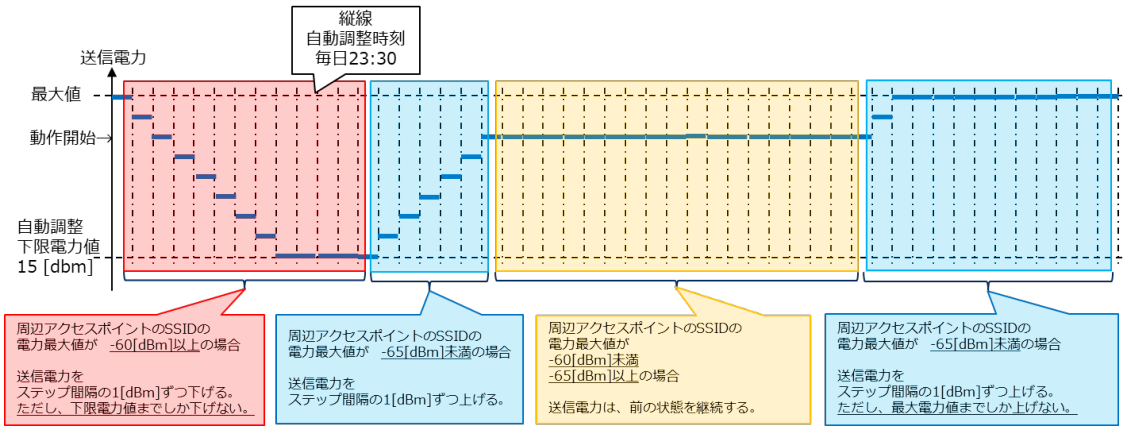
使用しているチャネルに関して、周辺アクセスポイントの同一チャネル電波強度情報を収集し、
周辺アクセスポイントの同一チャネルの電波強度に応じて、送信電力を調整できます。
無線インタフェース（radio0／radio1）ごとに、最大 2 個までスケジュールを設定することができます。
ただし、スケジュール設定時刻は、チャネル自動更新スケジュールと共通になります。

また、設定時刻の時点で、帰属無線クライアントがある場合、初期状態では送信電力自動調整を
行わない設定ですが、送信電力自動調整を強制的に行う設定も可能です。

送信電力自動調整を強制的に行う設定になっている場合、
設定時刻にいったん帰属が外れ、無線クライアントの再帰属が発生します。

本設定は、radio0 または radio1 のインタフェースコンフィグレーションモードにて設定が可能です。
以下は、radio0 インタフェースの設定例になります。

動作例



対象インタフェース	radio0
送信電力自動調整のスケジュール	23:30（channel-scan-schedule add TIME を使用） ※チャネル自動更新時刻と共通
送信電力最大値[dBm]	30（power level） ※国内の上限値範囲内での動作になります。

送信電力自動調整下限電力値[dBm] 15(power-scan-schedule low-limit-level)
周辺アクセスポイント SSID 電力監視レベル上限閾値[dBm]
-60(power-scan-schedule upper-threshold)
周辺アクセスポイント SSID 電力監視レベル下限閾値[dBm]
-65(power-scan-schedule lower-threshold)
送信電力の自動調整に使用するステップ間隔[dBm]
1(power-scan-schedule change-step)
周辺アクセスポイント SSID 電力監視の対象 BSSID
なし(no power-scan-schedule bssid-list)
送信電力自動調整強制実施 無効(no power-scan-schedule force)
送信電力自動調整機能 有効(power-scan-schedule enable)

動作例の設定

```
AP(config)# interface radio0          インタフェースコンフィグレーションモードに遷移
AP(config-if-radio0)# power level 30  送信電力最大値
                                      ※国内の上限値範囲内での動作になります。
AP(config-if-radio0)# channel-scan-schedule add 23:30
                                送信電力自動調整時刻 23:30 に設定
                                ※チャネル自動更新時刻と共通
AP(config-if-radio0)# power-scan-schedule low-limit-level 15
                                送信電力自動調整下限電力値を 15 に設定
AP(config-if-radio0)# power-scan-schedule upper-threshold -60
                                周辺アクセスポイント SSID 電力監視レベル
                                上限閾値を -60 に設定
AP(config-if-radio0)# power-scan-schedule lower-threshold -65
                                周辺アクセスポイント SSID 電力監視レベル
                                下限閾値を -65 に設定
AP(config-if-radio0)# power-scan-schedule change-step 1
                                送信電力の自動調整に使用するステップ間隔を 1 に設定
AP(config-if-radio0)# no power-scan-schedule bssid-list
                                周辺アクセスポイント SSID 電力監視の
                                対象 BSSID を設定しない
AP(config-if-radio0)# no power-scan-schedule force
                                帰属無線クライアントがある場合、
                                送信電力自動調整を実施しない
AP(config-if-radio0)# power-scan-schedule enable
                                送信電力自動調整スケジュール有効
AP(config-if-radio0)# !
AP(config)# write memory
```

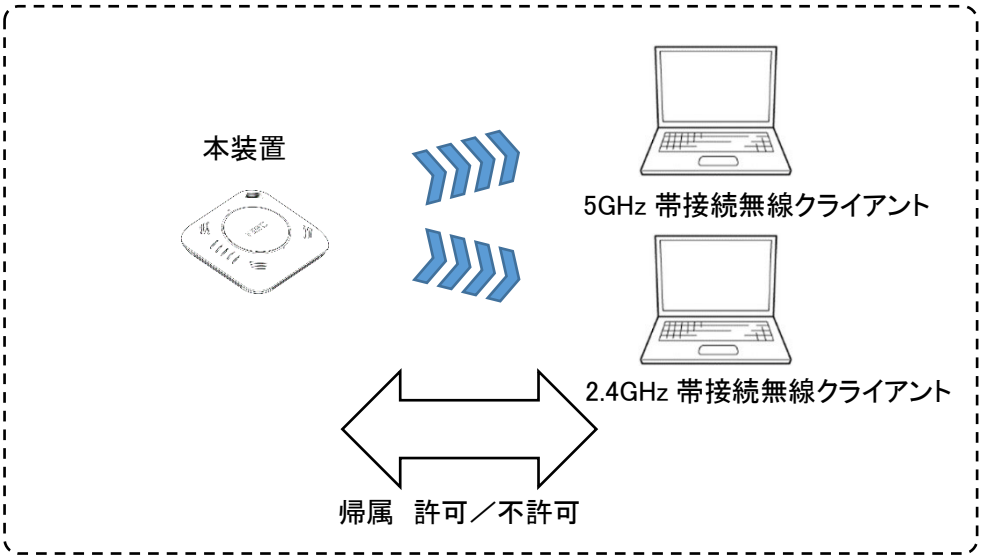
4.3.　設定事例 3　無線クライアントの帰属管理

無線クライアントの帰属管理は、
無線クライアント用 MAC アドレスフィルタリング機能を使用します。
設定／リスト変更／解除には、おのおの以下のステップを行います。
また、変更後、「write memory」を実行することで、適用されます。

＜設定＞
① MAC アクセスリストの登録
② フィルタの設定適用
③ 「write memory」実行

＜リスト変更（フィルタの設定適用済み）＞
① MAC アクセスリストの追加／削除
② 「write memory」実行

＜解除＞
① フィルタの設定無効
② MAC アクセスリストの削除（再度同じ内容で使用する場合は、削除不要）
③ 「write memory」実行



4.3.1. MAC アクセスリストを登録／削除する

MAC アドレスフィルタリング機能は、無線クライアントの帰属管理に使用します。
そのため、MAC アクセスリストならびに適用設定は、SSID 単位で行います。
5GHz 帯/2.4GHz 帯にて同一の SSID を使用している場合は、該当 SSID に設定すると
5GHz 帯/2.4GHz 帯両方に適用されます。

4.3.1.1. MAC アクセスリストに無線クライアントを登録する

登録対象 SSID	test
登録 MAC アドレス	AA:AA:AA:AA:AA:AA
	BB:BB:BB:BB:BB:BB
	E4:B3:18:A5:7B:E3

以下のコマンドにて、対象の無線クライアントを追加します。

```
AP(config)# ssid test
AP(config-ssid test)# mac access-list add AA:AA:AA:AA:AA:AA
AP(config-ssid test)# mac access-list add BB:BB:BB:BB:BB:BB
AP(config-ssid test)# mac access-list add E4:B3:18:A5:7B:E3
AP(config-ssid test)# !
AP(config)# write memory
```

4.3.1.2. MAC アクセスリストから無線クライアントを削除（個別）する

削除対象 SSID	test
削除 MAC アドレス	E4:B3:18:A5:7B:E3

以下のコマンドにて、対象の無線クライアントをリストから個別に削除します。

```
AP(config)# ssid test
AP(config-ssid test)# mac access-list del E4:B3:18:A5:7B:E3
AP(config-ssid test)# !
AP(config)# write memory
```

4.3.1.3. MAC アクセスリストから無線クライアントを削除（一括）する

削除対象 SSID	test
削除 MAC アドレス	登録している MAC アドレスすべて

以下のコマンドにて、リストに登録している無線クライアントの MAC アドレスを一括削除します。

```
AP(config)# ssid test
AP(config-ssid test)# no mac access-list
AP(config-ssid test)# !
AP(config)# write memory
```

4.3.2. MAC アクセスリストを適用する

SSID 単位で、MAC アクセスリストは、1 つずつ持つことができます。
登録した MAC アクセスリストに対して、

allow	:アクセスリストに登録した無線クライアントの接続を許可します。
deny	:アクセスリストに登録した無線クライアントの接続を不許可にします。
disable	:アクセスリストによるチェック機能を無効にします。

を行うことができます。

4.3.2.1. 登録した無線クライアントの帰属を許可する

mac access-list に登録した無線クライアントに帰属を許可します。

```
AP(config)# ssid test
AP(config-ssid test)# mac filter allow
AP(config-ssid test)# !
AP(config)# write memory
```

4.3.2.2. 登録した無線クライアントの帰属を不許可にする

mac access-list に登録した無線クライアントに帰属を不許可にします。

```
AP(config)# ssid test
AP(config-ssid test)# mac filter deny
AP(config-ssid test)# !
AP(config)# write memory
```

4.3.2.3. 登録した無線クライアントアクセスリストを無効にする

mac access-list を無効にします。
本設定を行っても、MAC アクセスリストの設定内容は、消去されません。

```
AP(config)# ssid test
AP(config-ssid test)# mac filter disable
AP(config-ssid test)# !
AP(config)# write memory
```

または、

```
AP(config)# ssid test
AP(config-ssid test)# no mac filter
AP(config-ssid test)# !
AP(config)# write memory
```

4.3.3. MAC アクセスリストの適用状態を確認する

下記コマンドにて、MAC アクセスリストの設定内容ならびに適用状態を確認できます。

```
AP(config)# show mac filter
```

アクセスリストおよび適用状態の設定後の読み出し例は次のとおりです。
以下の例は、5GHz 帯/2.4GHz 帯で、同一の SSID を使用して、許可設定を行った場合の内容になります。

```
AP(config)# show mac filter
[radio0]
SSID:test
  AccessType:allow
    aa:aa:aa:aa:aa:aa
    bb:bb:bb:bb:bb:bb
    e4:b3:18:a5:7b:e3

[radio1]
SSID:test2
  AccessType:allow
    aa:aa:aa:aa:aa:aa
    bb:bb:bb:bb:bb:bb
    e4:b3:18:a5:7b:e3
```

4.4.　設定事例 4　RADIUS サーバ認証の設定

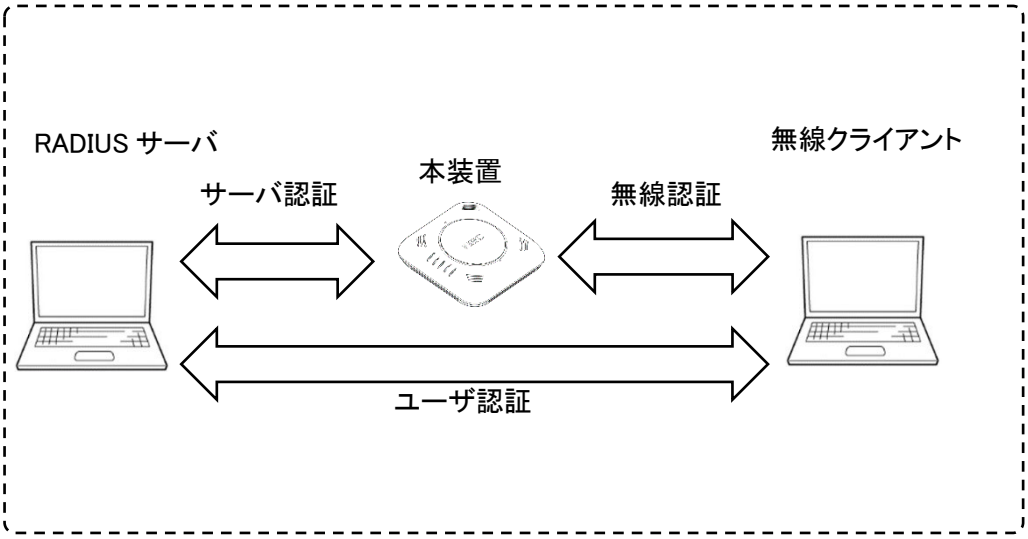
RADIUS サーバを用いて認証を行うための各種設定は、SSID 単位で行います。
ここでは、

サーバ認証　　RADIUS サーバと NA1500A 間の認証
無線認証　　無線クライアントと NA1500A 間の無線暗号化と認証

を説明します。

RADIUS サーバのユーザ認証は、各無線クライアントと RADIUS サーバ間で実施します。
無線クライアントのユーザ設定、RADIUS サーバ側の認証設定、ユーザ設定は、
ご使用になっている RADIUS サーバの説明書などを参照してください。

ソフトウェアバージョン 2.0 以降は、RADIUS サーバを 2 台まで接続可能です。



4.4.1. 使用するプライマリ RADIUS サーバを設定する

無線認証関連設定例は、以下のとおりです。

SSID 名	test_radius
無線クライアント許容台数	10 台
認証モード	WPA2 エンタープライズ-802.1X
暗号化	AES

サーバ認証関連設定例は、以下のとおりです。

RADIUS サーバの IPv4 アドレス	192.168.1.11
アカウンティングポート	ポート 1813
認証ポート	ポート 1812
最大送信回数（初回含む）	5 回
再送時のタイムアウト時間	3 秒
共有鍵が、平文 or 暗号	平文
事前共有鍵	87654321

SSID を作成し SSID コンフィグレーションモードにて設定します。
以下は最低限の設定になります。
接続先無線インタフェースならびに接続先 VLAN インタフェースなどに関する設定は、
「設定事例 2　無線インタフェースの利用」を参照してください。

```
AP(config)# ssid test_radius・・・・・・・・・・・・・・・・・・・・・・・・RADIUS サーバ認証用 SSID
AP(config-ssid test_radius)# max-associations 10・・・・・・無線クライアント接続許容台数
AP(config-ssid test_radius)# encryption mode wpa2 aes・・・・①
AP(config-ssid test_radius)# authentication type dot1x・・・・・①
                                                    無線クライアントとの認証／暗号設定
                                                    （WPA2 エンタープライズ-802.1X/AES）
AP(config-ssid test_radius)# radius host ip 192.168.1.11 ・・・
                                                        プライマリ RADIUS サーバの
                                                        IPv4 アドレス
                                    acct-port 1813 ・・アカウンティングポート
                                                        アカウンティング機能を使用し
                                                        ない場合は、0 を入力します。
                                                        本オプション省略時は、
```

前の状態を引き継ぎます。
auth-port 1812 ・・認証ポート
認証機能を使用しない場合
は、0 を入力します。
本オプション省略時は、
前の状態を引き継ぎます。
retransmit 5 ・・・・・最大送信回数（初回含む）[回]
timeout 3 ・・・・・・・再送時のタイムアウト時間[秒]
key 0 ・・・・・・・・・共有鍵が、平文か暗号か指定
暗号化は将来予定となります。
87654321・・・・・・・事前共有鍵
AP(config-ssid test_radius)# radio-device radio0・・・・5GHz 帯無線インタフェース使用
AP(config-ssid test_radius)# enable-ssid・・・・・・・・・・・・・SSID 有効
AP(config-ssid test_radius)# !
AP(config)# write memory

4.4.2. 使用するセカンダリ RADIUS サーバを設定する

ソフトウェアバージョン 2.0 以降は、RADIUS サーバを 2 台まで登録することができます。
また、「4.4.1.使用するプライマリ RADIUS サーバを設定する」を先に設定を行わないとセカンダリ RADIUS サーバを設定することはできません。

セカンダリ RADIUS サーバは、SSID コンフィグレーションモードにて設定します。
以下は最低限の設定になります。

```
AP(config)# ssid test_radius・・・・・・・・・・・・・・・・・・・・・・・・RADIUS サーバ認証用 SSID
AP(config-ssid test_radius)# radius secondary-host ip 192.168.1.11・・・・
                                                    セカンダリ RADIUS サーバの
                                                    IPv4 アドレス
                                  acct-port 1813 ・・アカウンティングポート
                                                    アカウンティング機能を使用し
                                                    ない場合は、0 を入力します。
                                                    本オプション省略時は、
                                                    前の状態を引き継ぎます。
                                  auth-port 1812 ・・認証ポート
                                                    認証機能を使用しない場合
                                                    は、0 を入力します。
                                                    本オプション省略時は、
                                                    前の状態を引き継ぎます。
AP(config-ssid test_radius)# radio-device radio0・・・・・・5GHz 帯無線インタフェース使用
AP(config-ssid test_radius)# enable-ssid・・・・・・・・・・・・・SSID 有効
AP(config-ssid test_radius)# !
AP(config)# write memory
```

4.4.3. RADIUS サーバへのアクセスブロックを設定する

ソフトウェアバージョン 2.0 以降は、RADIUS サーバを 2 台まで登録することができます。
RADIUS サーバを 2 台使用する場合に限りプライマリ RADIUS サーバへのアクセスブロックを設定することができます。
本設定値は、プライマリサーバ／セカンダリサーバで共通に使用します。
プライマリサーバで認証エラーとなった場合、設定した期間は、プライマリ RADIUS サーバとの認証を行わず、セカンダリサーバと認証を行います。
期間満了時にはプライマリサーバへ認証先の切り戻しを行います。
この設定はセカンダリサーバが設定されている場合にのみ有効です。

RADIUS サーバへのアクセスブロックは、SSID コンフィグレーションモードにて設定します。
以下は最低限の設定になります。

```
AP(config)# ssid test_radius・・・・・・・・・・・・・・・・・・・・・・・・RADIUS サーバ認証用 SSID
AP(config-ssid test_radius)# radius deadtime 10・・・・・・・・アクセスブロック時間 10 分
AP(config-ssid test_radius)# radio-device radio0・・・・・・5GHz 帯無線インタフェース使用
AP(config-ssid test_radius)# enable-ssid・・・・・・・・・・・・・SSID 有効
AP(config-ssid test_radius)# !
AP(config)# write memory
```

4.4.4. RADIUS サーバへの再認証間隔を設定する

RADIUS サーバへ再認証する時間間隔を設定します。
本設定値は、プライマリサーバ／セカンダリサーバで共通に使用します。

RADIUS サーバへの再認証間隔は、SSID コンフィグレーションモードにて設定します。
以下は最低限の設定になります。

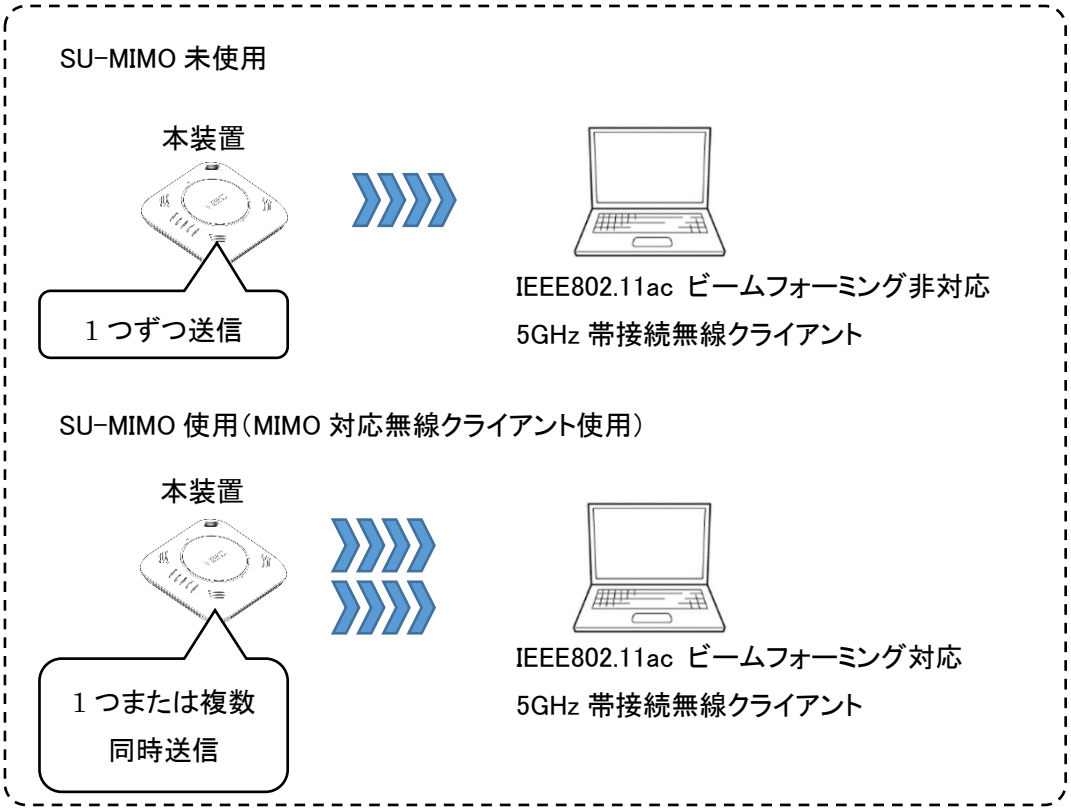
```
AP(config)# ssid test_radius・・・・・・・・・・・・・・・・・・・・・・・・RADIUS サーバ認証用 SSID
AP(config-ssid test_radius)# radius reauthentication 30・・再認証間隔時間  30 分
AP(config-ssid test_radius)# radio-device radio0・・・・・5GHz 帯無線インタフェース使用
AP(config-ssid test_radius)# enable-ssid・・・・・・・・・・・・・SSID 有効
AP(config-ssid test_radius)# !
AP(config)# write memory
```

4.5.　設定事例 5　送信ビームフォーミングの設定

本装置は、初期状態では、送信ビームフォーミング（SU-MIMO/MU-MIMO）が、無効設定になっています。
次の設定を行うことで、送信ビームフォーミングを有効にし、スループットを向上させることが可能です。
ただし、本機能を使用する場合、接続する無線クライアントも MIMO 機能を有する必要があります。
MIMO 機能に対応していない無線クライアントを使用する場合、スループットは向上せず、低下する場合があります。
また、本機能は、IEEE802.11ac 以外のモードでは、使用できません。

4.5.1. SU-MIMO を設定する

SU-MIMO 機能は、一度に 1 台の無線クライアントに対し、1 つまたは複数の送信を
同時に行うことができます。

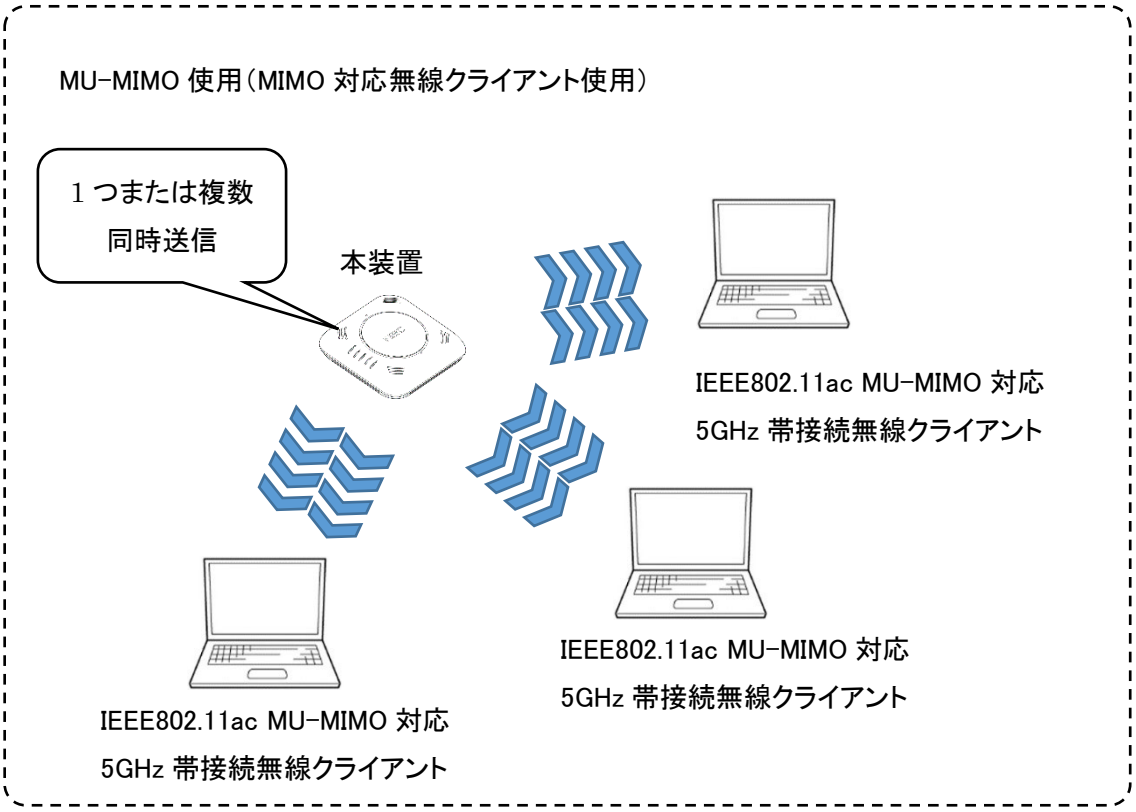


IEEE802.11ac を設定した radio0 インタフェースのみ設定が可能です。

AP(config)# interface radio0
AP(config-if-radio0)# tx-beamform-enable・・・・・・・SU-MIMO 有効
AP(config-if-radio0)# !
AP(config)# write memory

4.5.2. MU-MIMO を設定する

MU-MIMO は、一度に複数の無線クライアントに対し、1 つまたは複数の送信を
同時に行うことができます。



IEEE802.11ac を設定した radio0 インタフェースのみ設定が可能です。

```
AP(config)# interface radio0
AP(config-if-radio0)# tx-beamform-enable 3・・・・・・・MU-MIMO 有効
AP(config-if-radio0)# !
AP(config)# write memory
```

4.6.　設定事例 6　リンクインテグリティの設定

リンクインテグリティの機能を使用することで、

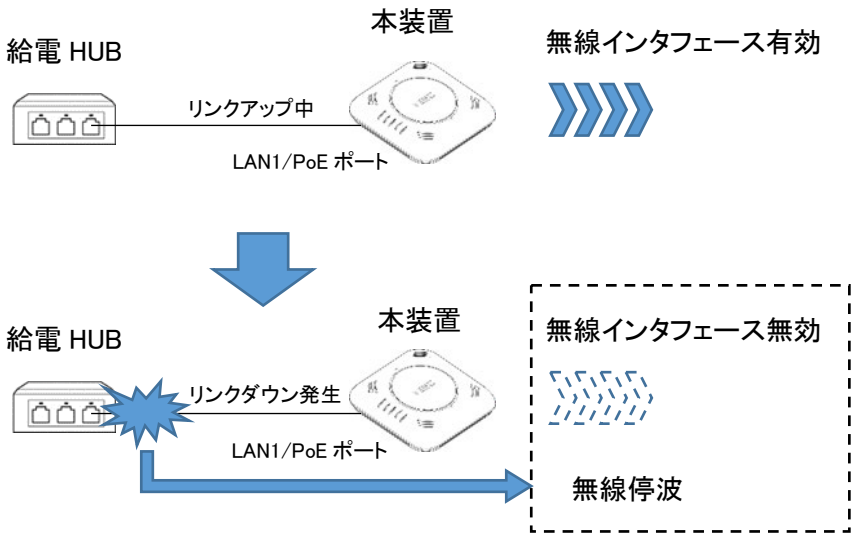
・有線インタフェースのリンク状態

・有線インタフェースに接続したホストとの通信状態

を監視し、無線インタフェースの有効／無効を連動して制御することができます。

有線インタフェース（LAN1/PoE ポート）のリンク状態と無線インタフェースの有効／無効の制御動作は以下のとおりです。

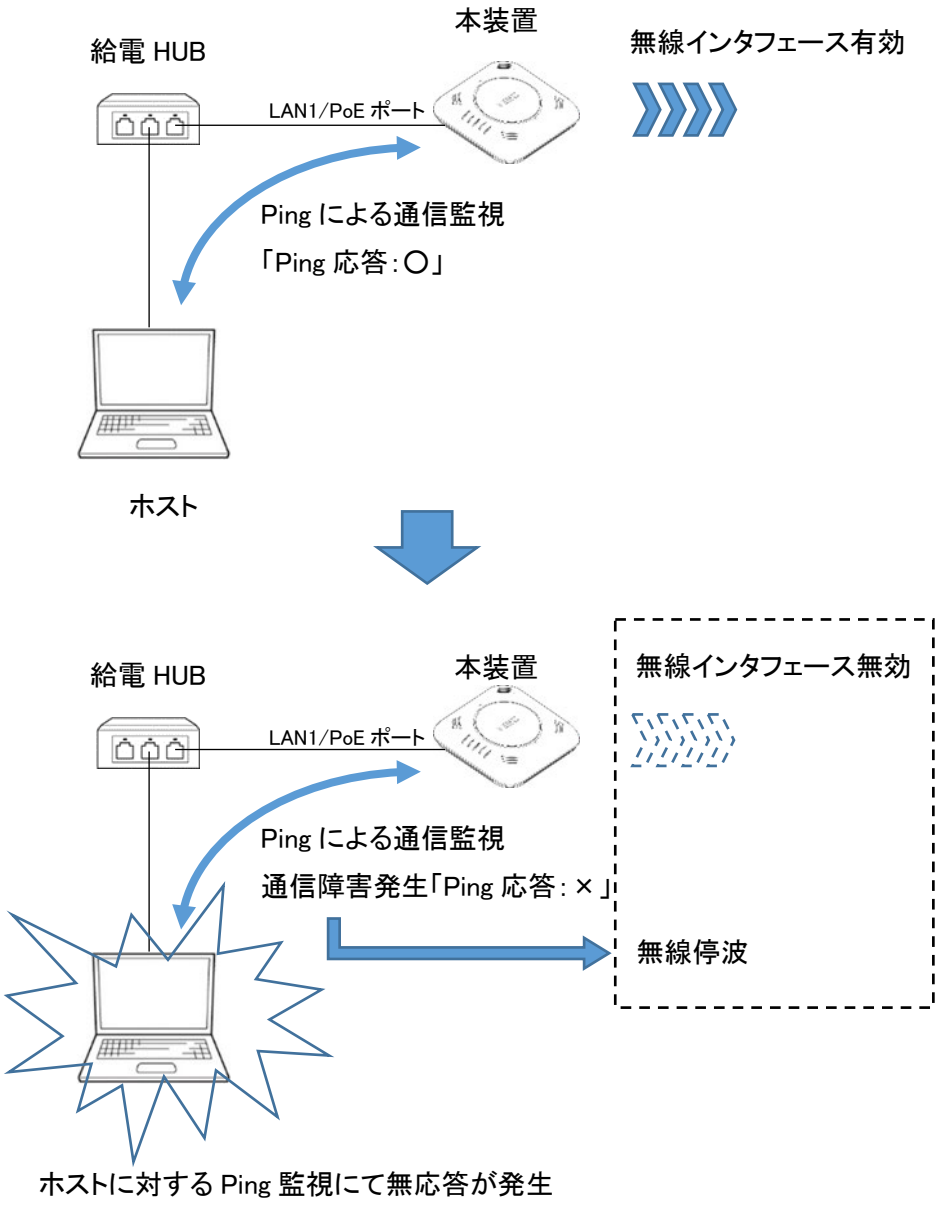
有線インタフェース（LAN1/PoE ポート）が動作中にリンクダウンが発生した場合



LAN1/PoE ポートのリンクダウンを検出すると
無線インタフェースを無効にし、無線を停波します。

有線インタフェースに接続したホストとの通信状態と無線インタフェースの有効／無効の制御動作は以下のとおりです。

有線インタフェース（LAN1/PoE ポート）にネットワーク経由で接続されたホストとの間を Ping にて通信状態監視中、ホストとの間で通信不通が発生した場合



4.6.1. イーサネットインタフェースのリンク監視を設定する

GigaEthernet インタフェースのリンク監視条件を設定します。
リンク監視条件の個別追加／個別削除および clear watchlist interface を行うことで、一括削除を行うことができます。
また、設定を残したまま機能の有効／無効の切り替えを行うことができます。

リンクインテグリティ動作開始条件

指定したインタフェースのリンクダウン継続状態が MONITOR-CYCLE 秒間継続した場合に動作を開始します。

対象インタフェースは GigaEthernet0 のみで、GigaEthernet1 は将来拡張予定です。

リンクインテグリティ動作解除条件

指定したインタフェースがリンクアップになった時点で動作を解除します。

本設定は、管理用 VLAN の VLAN インタフェースコンフィグレーションモードにて設定します。

```
AP(config)# interface vlan u
                    ・・・・・・・・管理用 VLAN インタフェースコンフィグレーションモード移行
AP(config-vlan u)# watchlist interface add  GigaEthernet0
                    ・・・・・・・監視対象のインタフェースを設定
AP(config-vlan u)# watchlist interface enable・・・・・・・リンク監視機能の有効設定
AP(config-vlan u)# !
AP(config)# write memory
```

4.6.2. 通信監視ホストのアドレスと監視条件を設定する

通信監視を行うホストの IPv4 アドレスまたはホスト名を、リストに登録します。
VLAN あたり 4 つまでホストの登録が可能です。
通信監視を行うホストの 個別追加／個別削除および clear watchlist host-ip を行うことで、一括削除を行うことができます。
また、設定した通信監視を行うホストの監視条件を watchlist host-monitor を行うことで、設定することができます。
ホストの通信監視は、設定を残したまま機能の有効／無効の切り替えを行うことができます。

本設定は、管理用 VLAN の VLAN インタフェースコンフィグレーションにて設定します。

```
AP(config)# interface vlan u
                    ・・・・・・・・管理用 VLAN インタフェースコンフィグレーションモード移行
AP(config-vlan u)# watchlist host-ip add 192.168.1.1・・・・・・・・・監視対象のホストを登録
AP(config-vlan u)# watchlist host-monitor monitor-cycle 30 monitor-retry 4
                    ・・・・・・・・・Ping 監視周期は、30 秒
                                     Ping 失敗時の再送回数は、4 回
                                     の場合の設定
AP(config-vlan u)# watchlist host-ip enable・・・・・・ホスト通信監視の有効設定
AP(config-vlan u)# !
AP(config)# write memory
```

4.6.3. 無線インタフェースの停止条件を設定する

リンク監視条件ならびに通信監視条件がマッチした場合の、無線側停止条件の有効／無効を設定することができます。
本設定を無効にしている場合は、リンク監視条件ならびに通信監視条件がマッチした場合でも無線側は、停止しません。
ただし、条件を検出した内容のログを残すことはできます。

本設定は、管理用 VLAN の VLAN インタフェースコンフィグレーションにて設定します。

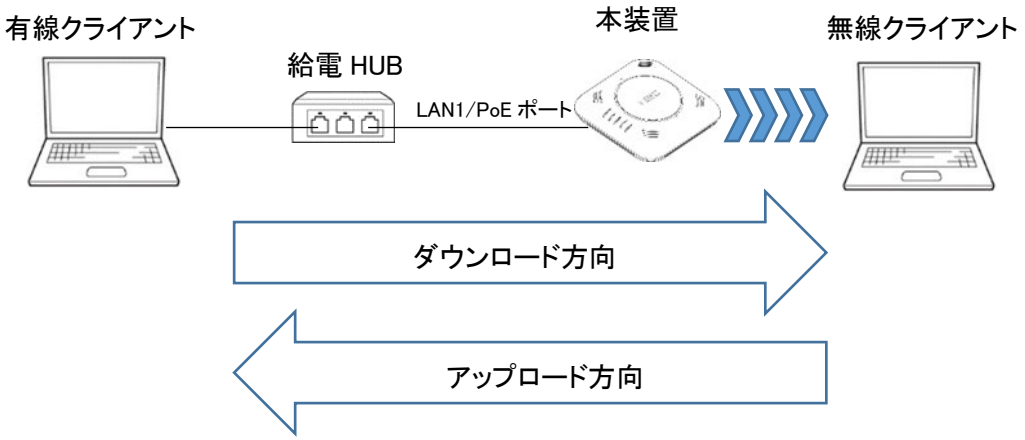
```
AP(config)# interface vlan u
                    ・・・・・・・・・管理用 VLAN インタフェースコンフィグレーションモード移行
AP(config-vlan u)# watchlist action shutdown
                    ・・・・・・・・・リンク監視条件ならびに通信監視条件がマッチした場合
                                      radio0（5GHz 帯）／radio1（2.4GHz 帯）
                                      両方のインタフェースを停止します。
AP(config-vlan u)# !
AP(config)# write memory
```

4.7.　設定事例 7 トラフィックシェーピングの設定

SSID 単位のトラフィックシェーピングを設定することができます。
シェーピングは、「total-upload」を使用して無線インタフェースの SSID から有線インタフェースへのアップロード帯域を指定できます。また、「total-download」を使用して有線インタフェースから無線インタフェースの SSID へのダウンロード帯域を設定することができます。
両方向の帯域設定をする場合は、「total-upload」と「total-download」を同時に使用します。

設定可能数は、以下のとおりです。
「total-upload TU（アップロード帯域シェーピング）」設定は、最大 8 つの SSID まで設定可能です。
「total-download TD（ダウンロード帯域シェーピング）」設定は、最大 8 つの SSID まで設定可能です。
使用する SSID が、radio-device both 設定し、2 つのインタフェースにて使用する場合は、使用数は、2 つとしてカウントします。

シェーピングの方向は以下のとおり



本設定は、SSID コンフィグレーションモードにて設定します。

```
AP(config)# ssid ict・・・・・・・・・・・・・・・・・SSID コンフィグレーションモードに移行
AP(config-ssid ict)# traffic-shaping total-upload 10000 total-download 20000
                                        ・・・・・・・・・アップロード帯域を 10Mbps に設定
                                                          ダウンロード帯域を 20Mbps に設定
                                                          省略時は、前の状態を継続します。
AP(config-ssid ict)# !
AP(config)# write memory
```

4.8.　設定事例 8　送信 AMPDU の設定

SSID の送信 AMPDU の有効／無効の設定ならびに有効時のサブフレーム数設定を行うことができます。
送信 AMPDU は、初期状態では有効になっていますが、無効にすることができます。

本設定は、SSID コンフィグレーションモードにて設定します。

```
AP(config)# ssid ict・・・・・・・・・・・・・・・・・・・・・・・・SSID コンフィグレーションモードに移行
AP(config-ssid ict)# no tx-ampdu-enable・・・・・送信 AMPDU　無効
AP(config-ssid ict)# !
AP(config)# write memory
```

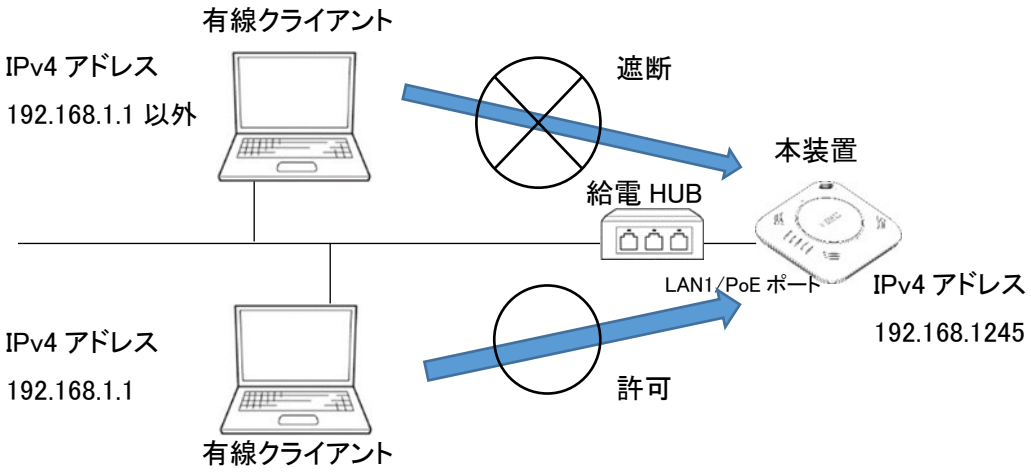
また、送信 AMPDU 有効時、のサブフレーム数を変更することができます。

```
AP(config)# ssid ict・・・・・・・・・・・・・・・・・・・・・・・・SSID コンフィグレーションモードに移行
AP(config-ssid ict)# tx-ampdu-subframes-limit 64・・・・・・サブフレーム数 64 に設定
                                                          （初期値は、64）
AP(config-ssid ict)# tx-ampdu-enable・・・・・・・・・・送信 AMPDU　有効
AP(config-ssid ict)# !
AP(config)# write memory
```

4.9.　設定事例 9　IP フィルタリングの設定

4.9.1.　特定の有線クライアント以外からの CLI へのアクセスを遮断する

GigaEthernet インタフェースに接続され、かつ管理用 VLAN に属しているすべての有線クライアントは、Telnet または SSH を用いて、CLI へアクセスを行うことができます。
ソフトウェアバージョン 3.0 以降では、特定の IPv4 アドレスの有線クライアント以外からのアクセスを遮断することができます。
以下は、GigaEthernet0 の管理用 VLAN に接続された IPv4 アドレス 192.168.1.1 の有線クライアントからは、CLI へのアクセスを許可するが、
192.168.1.1 以外の有線クライアントからのアクセスを遮断する場合の設定です。



アクセスリスト GE_PRMT_CLIENT に許可条件、GE_DNY_CLIENT に遮断条件を
設定します。
（※アクセスリスト名の使用可能文字数範囲は、1～15[文字]です。）

＜GigaEthernet インタフェースで使用する前提で条件を作成記載＞

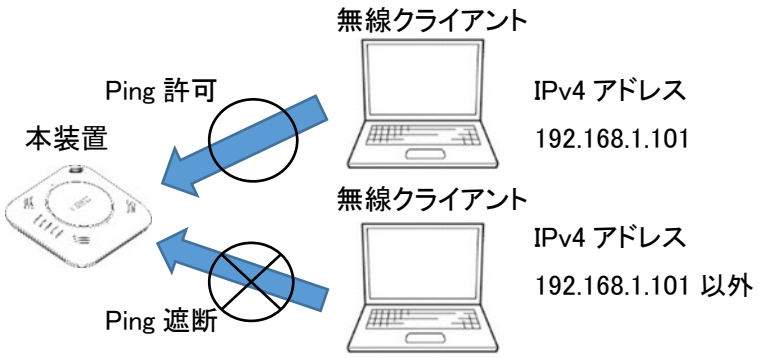
```
AP(config)# ip access-list GE_PRMT_CLIENT permit ip src 192.168.1.1/32 dest any
                                        ・・・192.168.1.1 への IP 通信許可
AP(config)# ip access-list GE_DNY_CLIENT deny ip src any dest any
                                        ・・・他のクライアントからの IP 通信遮断
```

＜GigaEthernet インタフェースの GigaEthernet0 に設定する場合＞

```
AP(config)# interface GigaEthernet0
AP(config-if-GigaEthernet0)# ip filter GE_PRMT_CLIENT 1 rcv
                                        ・・・シーケンス No.1 にて許可指定
AP(config-if-GigaEthernet0)# ip filter GE_DNY_CLIENT 2 rcv
                                        ・・・シーケンス No.2 にて遮断指定
AP(config-if-GigaEthernet0)# !
AP(config)# write memory
```

4.9.2. 無線クライアントから本装置への Ping を許可する

初期状態において、無線インタフェースに接続されているすべての無線クライアントは、本装置への Ping を許可されていません。
ソフトウェアバージョン 3.0 以降では、無線インタフェースに接続され、かつ管理用 VLAN に属しているすべてまたは、特定の無線クライアントから本装置への Ping を許可することができます。
以下は、radio0 の管理用 VLAN に接続された IPv4 アドレス 192.168.1.101 の無線クライアントからは、本装置への Ping を許可するが、
192.168.1.101 以外の無線クライアントからのアクセスを遮断する場合の設定です。



＜無線インタフェースで使用する前提で条件を作成記載＞
アクセスリスト RD_PRMT_CLIENT に許可条件を設定します。

```
AP(config)#
        ip access-list RD_PRMT_CLIENT permit icmp src 192.168.1.101/32 dest any
                                                ・・・192.168.1.101/32 からの Ping を許可
```

＜無線インタフェースの radio0 に設定する場合＞

```
AP(config)# interface radio0
AP(config-if-radio0)# ip filter RD_PRMT_CLIENT 1 rcv
                                                ・・・シーケンス No.1 にて許可指定
AP(config-if-radio0)# !
AP(config)# write memory
```

以下は、radio0 の管理用 VLAN に接続されたすべての無線クライアントから本装置への Ping を許可する場合の設定です。
（※アクセスリスト名の使用可能文字数範囲は、1～15[文字]です。）

＜無線インタフェースで使用する前提で条件を作成記載＞
アクセスリスト RD_PRMT_CLIENT に許可条件を設定します。

```
AP(config)# ip access-list RD_PRMT_CLIENT permit icmp src any dest any
                                        ・・・すべての無線クライアントからの Ping を許可
```

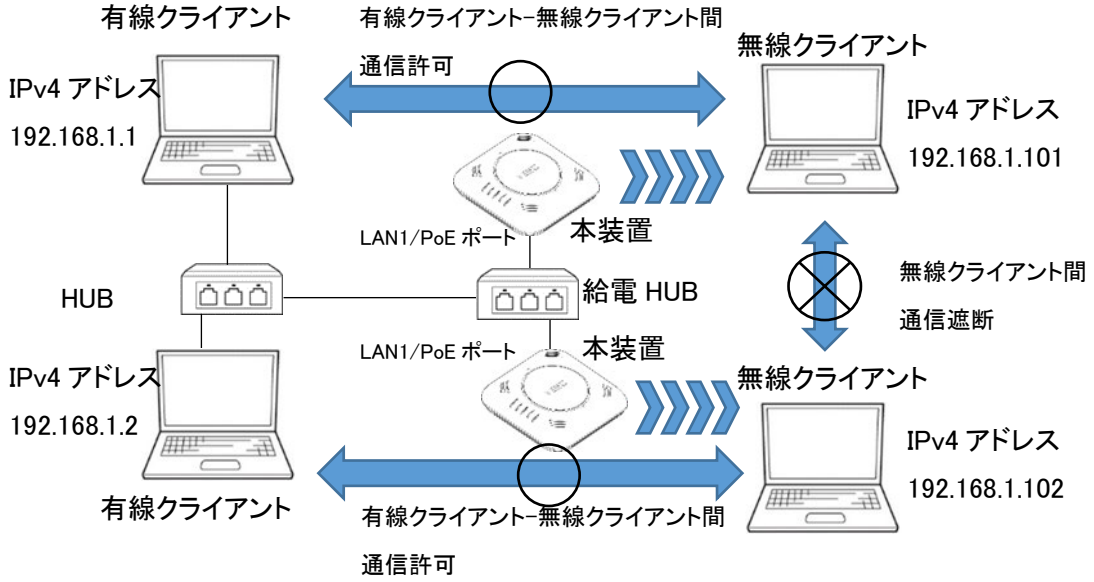
＜無線インタフェースの radio0 に設定する場合＞

```
AP(config)# interface radio0
AP(config-if-radio0)# ip filter RD_PRMT_CLIENT 1 rcv
                                        ・・・シーケンス No.1 にて許可指定
AP(config-if-radio0)# !
AP(config)# write memory
```

4.9.3. 無線クライアントと有線クライアント間のみ通信を許可する

※インタフェースに対して in または、out のフィルタを設定する場合、注意が必要です。
ip access-list コマンドにて、ip 指定、または、udp 指定にてフィルタをかける場合は、
以下設定例のとおり、双方向にて設定を行う必要があります。

以下は、同一 VLAN 内に NA1500A を 2 台接続し、有線クライアントは HUB を経由して 2 台の NA1500A に接続、そして無線クライアントは、おのおのの NA1500A に 1 台ずつ接続された環境において、無線クライアントからは、有線クライアント(192.168.1.1/192.168.1.2)への通信を許可するが無線クライアント間の通信は遮断する場合の設定です。



各装置の無線インタフェースに同一の内容を設定します。
（アクセスリスト名の使用可能文字数範囲は、1～15[文字]です。）
アクセスリスト RD_OUT_PRMT／RD_IN_PRMT に許可条件、
アクセスリスト RD_OUT_ALL_DNY／RD_IN_ALL_DNY に遮断条件を
設定します。
（※アクセスリスト名の使用可能文字数範囲は、1～15[文字]です。）

＜無線インタフェースで使用する前提で条件を作成記載＞

```
AP(config)# ip access-list RD_IN_PRMT permit ip src any dest 192.168.1.1/32
```
・・・・無線インタフェースでの有線クライアント（192.168.1.1/32）への通信の受信許可
```
AP(config)# ip access-list RD_OUT_PRMT permit ip src 192.168.1.1/32 dest any
```
・・・・無線インタフェースでの有線クライアント（192.168.1.1/32）からの通信の送信許可
```
AP(config)# ip access-list RD_IN_PRMT permit ip src any dest 192.168.1.2/32
```
・・・・無線インタフェースでの有線クライアント（192.168.1.2/32）への通信の受信許可
```
AP(config)# ip access-list RD_OUT_PRMT permit ip src 192.168.1.2/32 dest any
```
・・・・無線インタフェースでの有線クライアント（192.168.1.2/32）からの通信の送信許可
```
AP(config)# ip access-list RD_IN_ALL_DNY deny ip src any dest any
```
・・・・無線インタフェースでの他の有線クライアントへの通信の受信遮断
```
AP(config)# ip access-list RD_OUT_ALL_DNY deny ip src any dest any
```
・・・・無線インタフェースでの他の有線クライアントからの通信の送信遮断

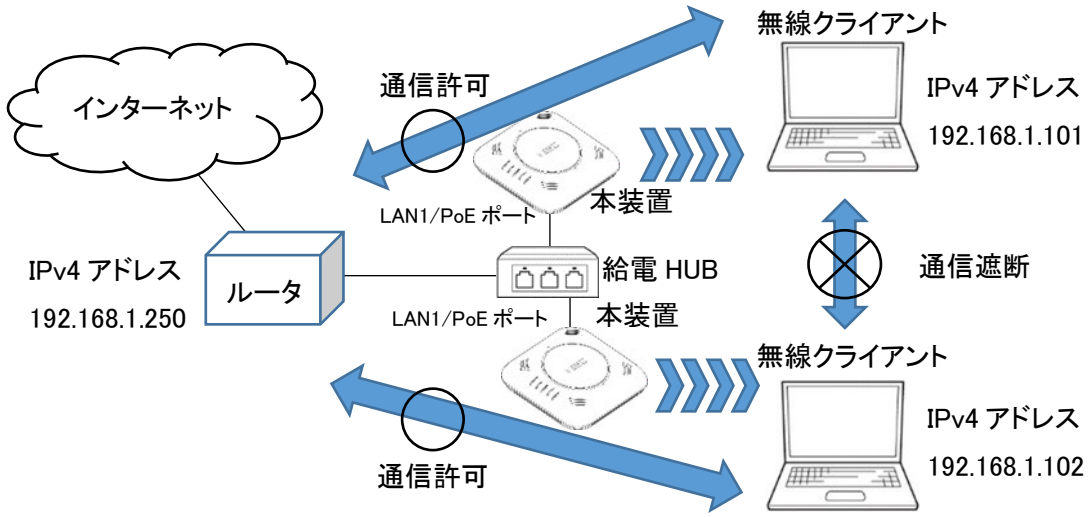
＜無線インタフェースの radio0 に設定する場合＞

```
AP(config)# interface radio0
AP(config-if-radio0)# ip filter RD_IN_PRMT 1 in
```
・・・シーケンス No.1 にて許可指定
```
AP(config-if-radio0)# ip filter RD_OUT_PRMT 2 out
```
・・・シーケンス No.2 にて許可指定
```
AP(config-if-radio0)# ip filter RD_IN_ALL_DNY 3 in
```
・・・シーケンス No.3 にて遮断指定
```
AP(config-if-radio0)# ip filter RD_OUT_ALL_DNY 4 out
```
・・・シーケンス No.4 にて遮断指定
```
AP(config-if-radio0)# !
AP(config)# write memory
```

4.9.4. 無線クライアントからルータを経由した通信のみを許可する

※インタフェースに対して in または、out のフィルタを設定する場合、注意が必要です。
ip access-list コマンドにて、ip 指定、または、udp 指定にてフィルタをかける場合は、
以下設定例のとおり、双方向にて設定を行う必要があります。

以下は、同一 VLAN 内に NA1500A を 2 台接続し、ルータは HUB を経由して 2 台の NA1500A に接続、そして無線クライアントは、おのおのの NA1500A に 1 台ずつ接続された環境において、無線クライアント(192.168.1.101/192.168.1.102)からは、ルータ(192.168.1.250)を経由した通信(インターネットなどへの通信)を許可するが無線クライアント間の通信は遮断する場合の設定です。
(各無線クライアントに設定する IPv4DNS サーバ/IPv4 ゲートウェイアドレスがルータの IPv4 アドレスの場合)



各装置の無線インタフェースに同一の内容を設定します。
アクセスリスト RD_OUT_PRMT／RD_IN_PRMT に許可条件、
アクセスリスト RD_OUT_ALL_DNY／RD_IN_ALL_DNY に遮断条件を
設定します。
（※アクセスリスト名の使用可能文字数範囲は、1～15[文字]です。）

＜無線インタフェースで使用する前提で条件を作成記載＞

AP(config)# ip access-list RD_IN_PRMT permit ip src any dest 192.168.1.250/32
　　・・・無線インタフェースでのルータ（192.168.1.250/32）へ通信の受信許可
AP(config)# ip access-list RD_OUT_PRMT permit ip src 192.168.1.250/32 dest any
　　・・・無線インタフェースでのルータ（192.168.1.250/32）からの通信の送信許可
AP(config)# ip access-list RD_IN_ALL_DNY deny ip src any dest 192.168.1.0/24
　　・・・無線インタフェースでの指定サブネットへの通信の受信遮断
AP(config)# ip access-list RD_OUT_ALL_DNY deny ip src 192.168.1.0/24 dest any
　　・・・無線インタフェースでの指定サブネットから通信の送信遮断

＜無線インタフェースの radio0 に設定する場合＞

AP(config)# interface radio0
AP(config-if-radio0)# ip filter RD_IN_PRMT 1 in
　　・・・シーケンス No.1 にて許可指定
AP(config-if-radio0)# ip filter RD_OUT_PRMT 2 out
　　・・・シーケンス No.2 にて許可指定
AP(config-if-radio0)# ip filter RD_IN_ALL_DNY 3 in
　　・・・シーケンス No.3 にて遮断指定
AP(config-if-radio0)# ip filter RD_OUT_ALL_DNY 4 out
　　・・・シーケンス No.4 にて遮断指定
AP(config-if-radio0)# !
AP(config)# write memory

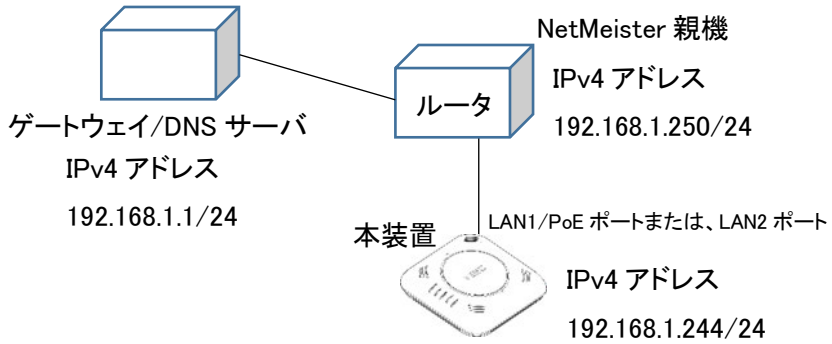
4.10.　設定事例 10　NetMeister クライアントの設定

4.10.1. NetMeister クライアント設定を手動で実施

※本機能は、あらかじめ「clock」コマンド または時刻同期機能を使用して時刻設定
　する必要があります。

※NetMeister クライアント機能は、集中管理クライアント機能と同時に使用できません。

NetMeister クライアント機能を使用するためには、NetMeister 親機となる機器が必要です。
以下は、NetMeister 親機（ルータ）を使用した場合の設定になります。



本装置の NetMeister 親機側に NetMeister 関連設定がされている必要があります。
本構成における設定例は、以下のとおりです。

```
AP(config)# hostname NA1500A-1      ・・・自ホスト名を固有なものに設定
AP(config)# nm enable               ・・・NetMeister クライアント機能を有効に設定
                                        ※集中管理クライアント機能が
                                          無効（no mt enable）になっている必要が
                                          あります。有効（mt enable）の場合、
                                          エラーになります。
AP(config)# nm account abcdefg password plain test12345678
                                    ・・・NetMeister 登録済みの GROUP-ID とパスワードを登録
                                        【注意】パスワードは、推測困難な文字列の
                                              組み合わせにて設定してください。
```

```
AP(config)# nm parent ip 192.168.1.250 port 443
                                    ・・・NetMeister 親機の IPv4 アドレスおよびポート番号設定
AP(config)# nm https-server ip port 443          ・・・自ポート番号を設定
AP(config)# no nm proxy                  ・・・Proxy 経由の接続の場合指定
AP(config)# no nm suppress-feature alarm
                                    ・・・アラーム送信を抑制しない場合の設定
```

本装置を固定アドレスにて NetMeister クライアント機能を使用する場合、
NetMeister 親機が指定する IPv4 ゲートウェイならびに IPv4DNS サーバを本装置にも
設定する必要があります。

```
AP(config)# interface vlan u                    ・・・Untagged-VLAN を使用する場合
AP(config-vlan u)# ip address 192.168.1.244/24     ・・・本装置 IPv4 アドレス
AP(config-vlan u)# ip route 192.168.1.1            ・・・IPv4 ゲートウェイアドレス
AP(config-vlan u)# dns server 192.168.1.1          ・・・IPv4DNS サーバアドレス
AP(config-vlan u)# vlan enable
AP(config-vlan u)# !
AP(config)# write memory
```

4.10.2. NetMeister クライアント設定をゼロタッチプロビジョニングで実施

NetMeister クライアント機能を使用するためには、NetMeister 親機となる機器が必要です。
NetMeister クライアント設定をゼロタッチプロビジョニング機能にて自動的に実施する場合、
事前に以下の設定が必要です。

(1) NetMeister サーバへ以下の登録を行う必要があります。
事前に以下の情報を準備します。
・ゼロタッチプロビジョニングを行いたい NA1500A のシリアル番号と MAC アドレス
・ゼロタッチプロビジョニングを行いたい NA1500A 用のコンフィグファイル

【注意】
ゼロタッチプロビジョニングにて使用する NA1500A のコンフィグファイルには、
「admin-name」コマンドを使用した管理者アカウントのユーザ名とパスワードを設定する
記載が必要です。
「admin-name」コマンドの記載がない場合は、ゼロタッチプロビジョニング動作に失敗し、
NA1500A の OPT-LED が赤点滅して通知します。
また、記載した「admin-name」コマンドパラメータの使用可能文字や文字数範囲などが、
条件に一致しない場合、管理者アカウントのユーザ名とパスワードを設定できません。

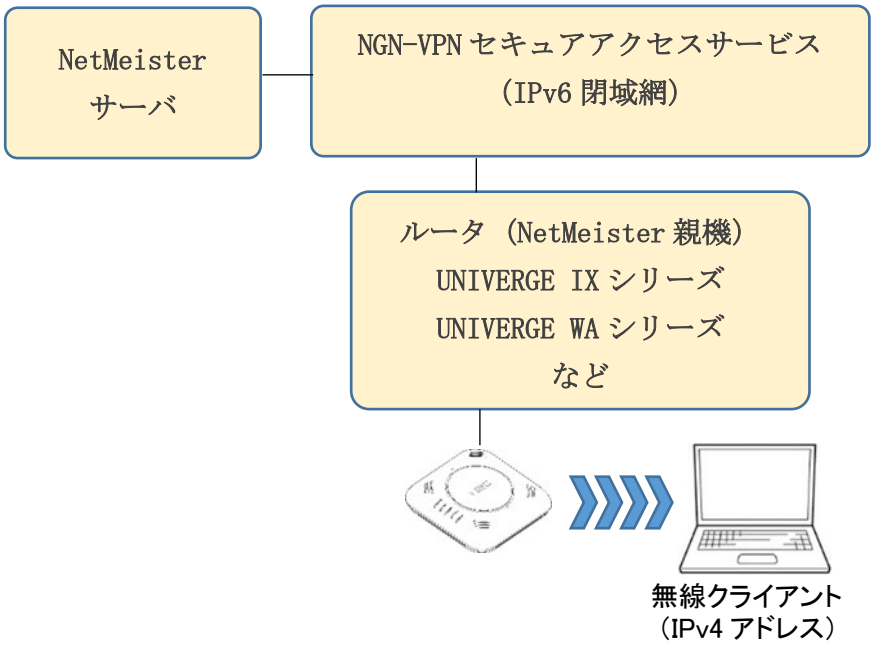
NetMeister サーバへの登録の流れは以下のとおりです。
※詳細は、NetMeister マニュアルの「ゼロタッチプロビジョニング設定」を参照してください。
・ゼロタッチプロビジョニングを使用する NA1500A の装置情報の登録
・ゼロタッチプロビジョニングを使用して設定する NA1500A 用のコンフィグのアップロード
・ゼロタッチプロビジョニングを使用する NA1500A の装置情報とコンフィグの紐づけ

(2) NetMeister 親機（ルータ）へ以下の設定を行う必要があります。
・NetMeister 親機（ルータ）が使用する NetMeister に接続していること
・NetMeister 親機（ルータ）の DHCP サーバ機能を有効に設定していること
・NetMeister 親機（ルータ）の NetMeister 子機用ゼロタッチプロビジョニング機能を有効に
設定しておくこと

(3) NA1500A は、以下の状態である必要があります。
ゼロタッチプロビジョニングにて NA1500A へコンフィグ自動設定を行う場合は、
対象の NA1500A を工場出荷状態にして、ケーブルを接続する必要があります。
「erase」コマンドまたは、RESET スイッチ長押しにて、工場出荷状態にすることができます。

4.10.3. NGN-VPN セキュアアクセスサービスの IPv6 閉域網の利用

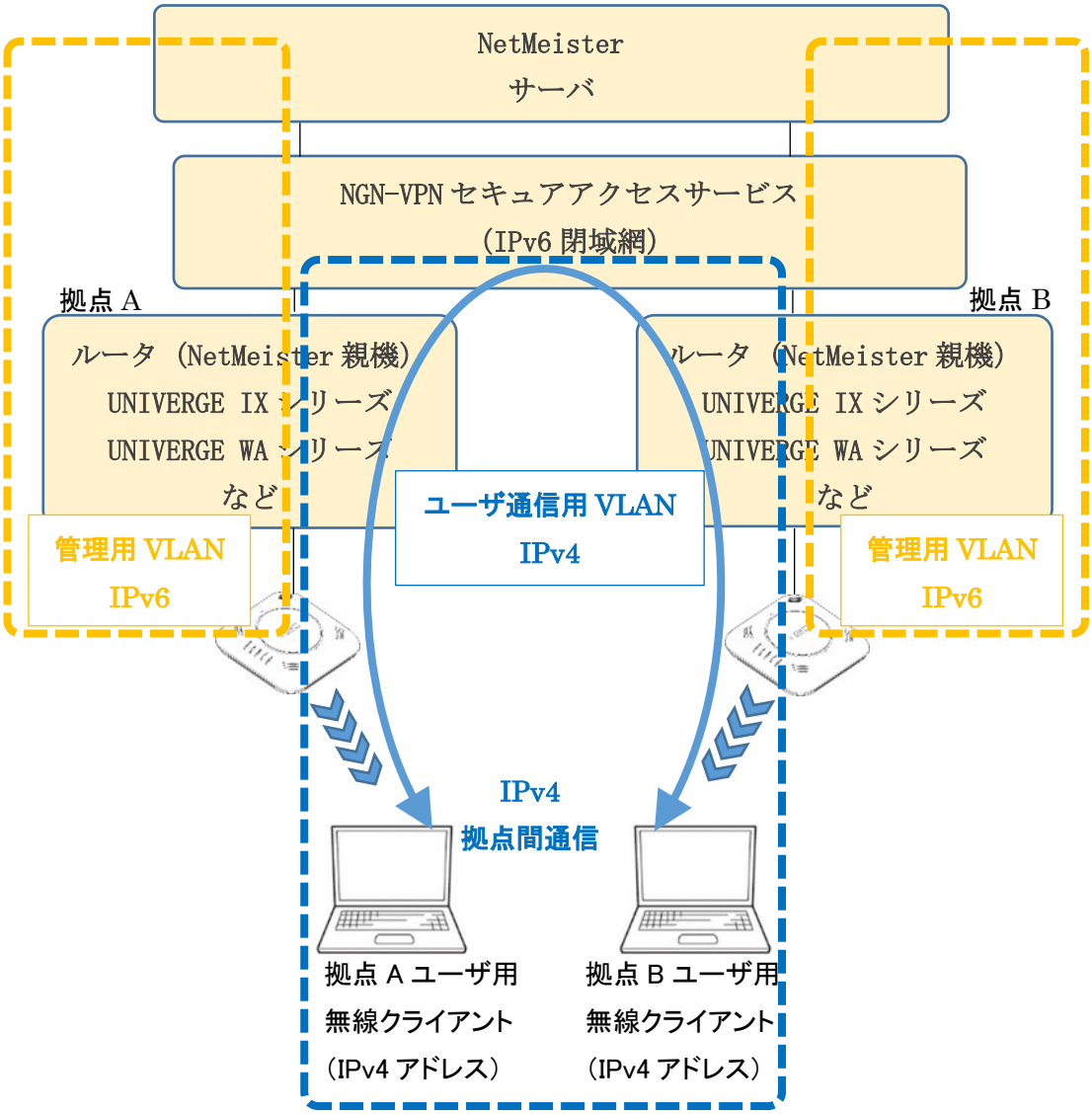
NGN-VPN セキュアアクセスサービスの IPv6 閉域網を使用して NetMeister クライアント機能を利用することができます。
NetMeister 親機には、UNIVERGE IX シリーズ/UNIVERGE WA シリーズなどを使用する必要があります。
NGN-VPN セキュアアクセスサービス(IPv6 閉域網)対応の機能を使用すると、
NA1500A と NetMeister サーバの間および NetMeister 親機(UNIVERGE IX シリーズ/UNIVERGE WA シリーズなど)と NetMeister サーバの間は、IPv6 にて制御通信が可能となります。
ただし、NetMeister 親機と NA1500A 間の制御通信は、IPv4 にて行われます。
NA1500A に無線接続した無線クライアントは、IPv4 でのみ利用が可能です。



(1) NetMeister 親機および NA1500A へ管理用 VLAN とユーザ通信用の VLAN 登録を行う必要があります。

管理用 VLAN は、NetMeister サーバと NA1500A の間の IPv6 制御通信に使用します。

ユーザ通信用 VLAN は、無線クライアントなどのユーザ通信のために使用します。



(2) NGN-VPN セキュアアクセスサービスの IPv6 閉域網対応の設定を行う必要があります。

・IPv6 の有効設定コマンド

ipv6 enable(ソフトウェア 8.0 以降では、初期状態で有効です。)

・NetMeister のクライアント機能 IPv6 閉域網対応設定コマンド

nm enable ipv6

(3) IPv6 閉域網内にて時刻同期を可能とする設定を行う必要があります。

閉域網の場合、網外部の NTP サーバを利用することはできません。

時刻同期を行うためには、閉域網内にローカルの NTP サーバを用意するか NetMeister との制御通信から時刻情報を抽出し利用する必要があります。

NetMeister との制御通信から時刻情報を抽出利用するためには、以下の設定が必要です。

ntp enable nm

本設定の場合、NetMeister との制御通信から抽出した時刻情報と本装置の時刻が、10 分以上ずれた場合のみ同期をします。

また、ローカルにある NTP サーバとの併用はできません。

(4) NGN-VPN セキュアアクセスサービス(IPv6 閉域網)を使用する場合、NetMeister へ追加の設定を行う必要があります。

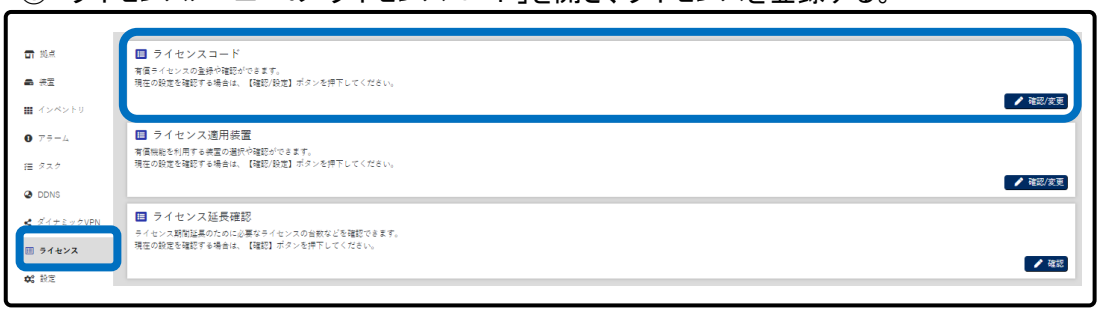
NetMeister のライセンスに関する追加設定手順は以下のとおりです。

※NetMeister へのログインなど基本操作は、NetMeister マニュアルを参照してください。

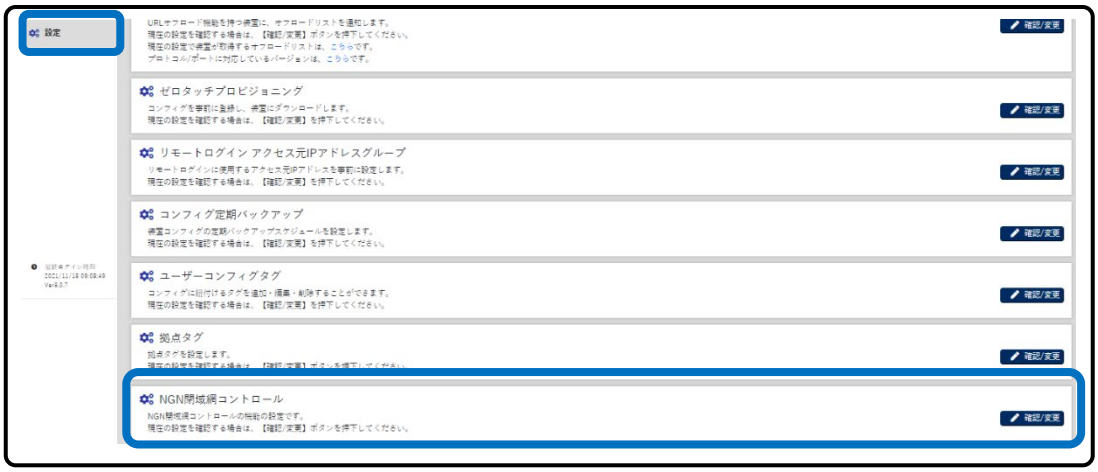
＜ライセンス登録を行って設定する場合＞

ご利用には、事前にライセンスを用意する必要があります。

① ライセンスメニューの「ライセンスコード」を開き、ライセンスを登録する。



② 設定メニューの「NGN 閉域網コントロール」を開き、NGN 閉域網コントロールを有効にする。

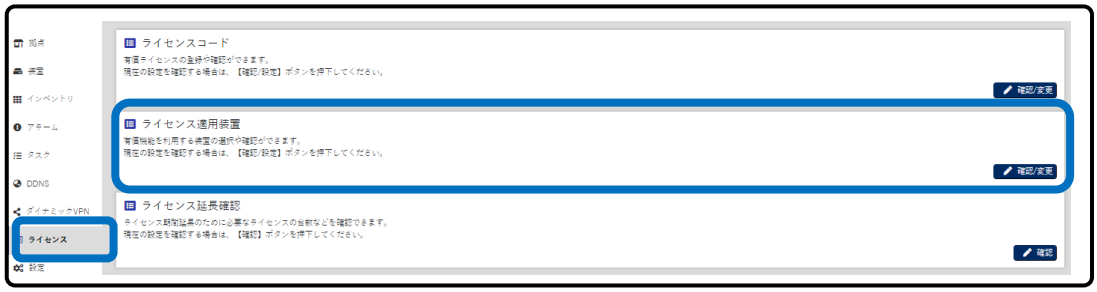


③ NA1500A を装置登録する。

追加する NA1500A へ NetMeister 関連の設定を行い、ネットワークへ接続します。

設定内容に問題がなければ、装置一覧画面に該当の NA1500A が追加表示されます。

④ ライセンスメニューの「ライセンス適用装置」を開き、NA1500A へライセンスを適用する。



＜ライセンスを使用せずに Prime トライアルを利用する場合＞

① NA1500A を装置登録する。

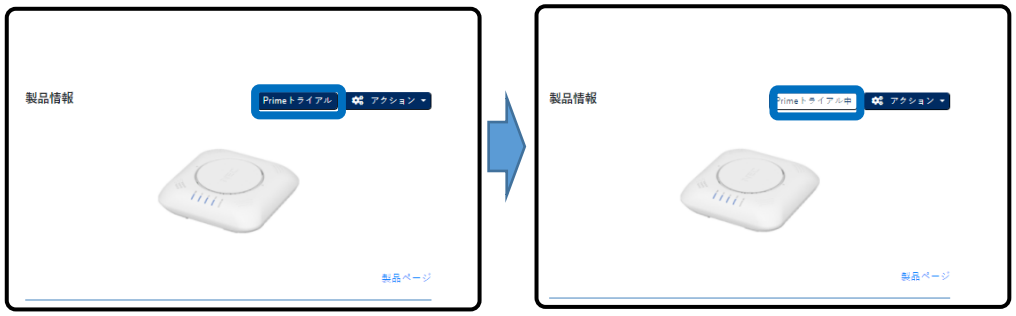
追加する NA1500A へ NetMeister 関連の設定を行い、ネットワークへ接続します。

設定内容に問題がなければ、装置一覧画面に該当の NA1500A が追加表示されます。

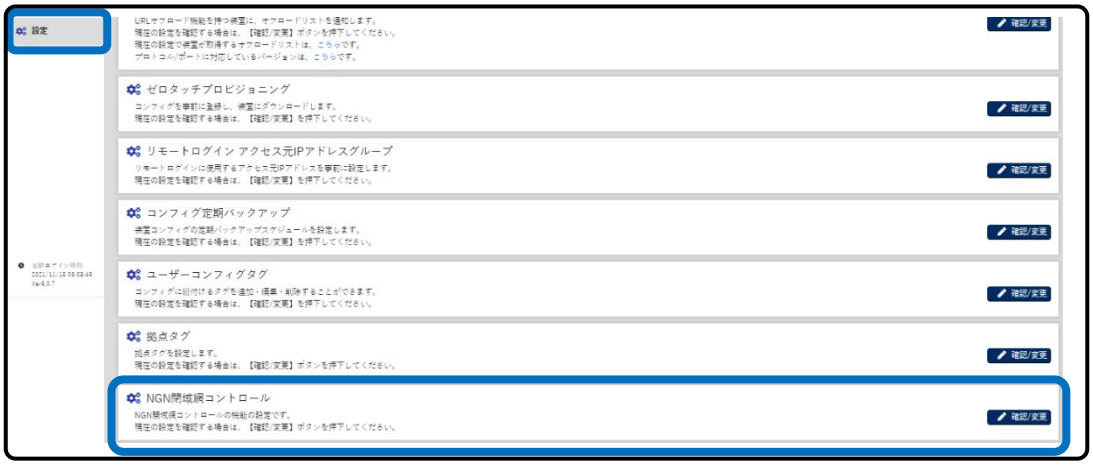
② NA1500A の Prime トライアルを利用開始する。

NA1500A 装置概要画面の「Prime トライアル」ボタンを押して、Prime トライアルの利用を開始します。

利用開始すると本ボタンの表示が、「Prime トライアル中」に変わります。



③ 設定メニューの「NGN 閉域網コントロール」を開き、NGN 閉域網コントロールを有効にする。



(5) NGN-VPN セキュアアクセスサービスを無償サービスから有償サービスへ切り替えを行う場合の注意事項

NA1500A がすでに NetMeister へ接続を行っている状態で、NetMeister のサービスを無償サービスから有償サービスへ切り替えを行った場合、NA1500A で有償サービスが利用可能になるためには以下のいずれかの条件を満たす必要があります。

・通常は、NetMeister 子機認証周期（最大 1 時間）が実行されたのち利用可能になります。

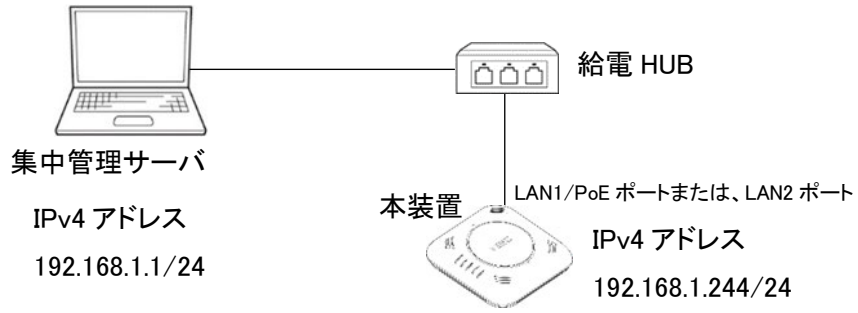
・コマンドにて NA1500A を再起動して NetMeister 子機認証を実行することで利用可能になります。

4.11. 設定事例 11 集中管理クライアントの設定

※集中管理クライアント機能は、NetMeister クライアント機能と同時に使用できません。

集中管理クライアント機能を使用するためには、集中管理サーバが別途必要です。

以下は、集中管理サーバを同一サブネット内で使用した場合の設定になります。



本構成における設定例は、以下のとおりです。

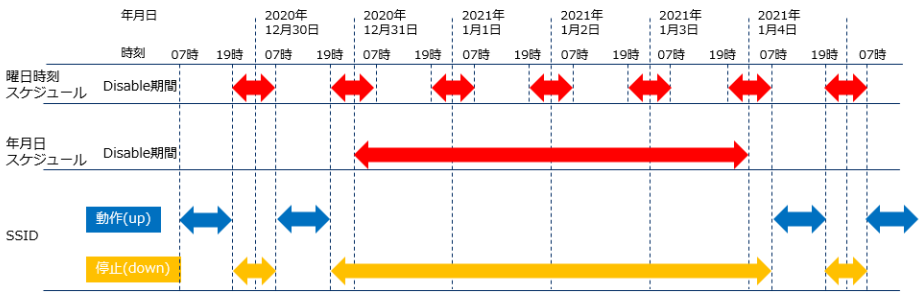
```
AP(config)# mt enable                    ・・・集中管理クライアント機能を有効に設定
                                               ※NetMeister クライアント機能が
                                                 無効(no nm enable)になっている
                                                 必要があります。
                                                 有効(nm enable)の場合、
                                                 エラーになります。
AP(config)# mt server ip 192.168.1.1     ・・・集中管理 サーバのアドレスを設定
AP(config)# mt reg-interval 15           ・・・集中管理サーバへ送信する周期情報の
                                                 送信間隔を設定(初期値は、15)
AP(config)# mt http-server ip port 10080
                                         ・・・自ポート番号を設定(初期値は、10080)
```

4.12.　設定事例 12　SSID 停止スケジュールの設定

※本機能は、あらかじめ「clock」コマンド　または時刻同期機能を使用して時刻設定
　する必要があります。
※本機能は、バンドステアリング（ロードバランス）機能と同時に使用できません。

年月日および、曜日時刻を指定することで、指定した期間 SSID を停止します。
SSID 単位で、停止するスケジュール設定およびスケジュールの有効／無効を設定します。

動作例
下記のとおり、曜日時刻スケジュールまたは年月日スケジュールのいずれかが該当する期間、
SSID を停止します。



SSID 名　　test_5G
SSID 停止期間設定　　曜日時刻　毎日 19 時～翌 7 時停止
　　年月日　　2020 年 12 月 31 日～2021 年 1 月 3 日停止

動作例の設定

SSID コンフィグレーションモードにて設定します。

AP(config)# ssid test_5G
AP(config-ssid test_5G)# ssid-disable-schedule add start-day-of-week everyday start-time 19:00 end-day-of-week everyday end-time 07:00
・・・・・・毎日 19 時～翌 7 時まで停止
AP(config-ssid test_5G)# ssid-disable-schedule add start-date 2020 12 31 end-date 2021 1 3
・・・・・・2020 年 12 月 31 日～2021 年 1 月 3 日は終日停止
AP(config-ssid test_5G)# ssid-disable-schedule enable
・・・・・・SSID 停止スケジュール有効
AP(config-ssid test_5G)# !
AP(config)# write memory

4.13.　設定事例 13　バンドステアリング（ロードバランス）の設定

※本機能は、SSID 停止スケジュール機能と同時に使用できません。

バンドステアリングは、SSID 単位で、有効／無効を指定します。
また、対象の SSID が、radio0（5GHz 帯）と radio1（2.4GHz 帯）の両方で有効になっている必要があります。

バンドステアリングを有効にすることで

Pre-association steering 機能

Idle post-association steering 機能

Active post-association steering 機能

すべての機能が有効になります。

種類	Pre-association steering	Idle post-association steering	Active post-association steering
概要	新たに帰属しようとする無線クライアントを過負荷になっていないバンドに誘導帰属します。	既に帰属している無線クライアントがIEEE802.11vをサポートしている場合、アップリンクデータ（keep alive相当）を監視しています。 アップリンクデータ通信を行っていない無線クライアントに対しバンドステアリングします。	既に帰属している無線クライアントがIEEE802.11kとIEEE802.11vをサポートしている場合、 データ通信中、 ・無線クライアントへの送信レート ・RSSI値 ・移動先バンドの通信負荷 により指定したバンドへステアリングします。
パラメータ バンドステアリング条件	既に帰属している各バンドの通信負荷量 （１分間継続していること）	無線子機がIEEE802.11vに対応していること	無線子機がIEEE802.11vとIEEE802.11k両方に対応していること
	新たに帰属しようとする無線クライアントのRSSI	ステアリング対象の無線クライアントのSSIDの両バンドが一定時間無通信の場合 （１０秒間継続していること）	2.4GHz帯へ帰属中のステアリング対象の無線クライアントの場合、 2.4GHz帯から5GHz帯へのバンド遷移は、 以下①または②のいずれかの条件を満たすこと ①無線クライアントへの送信レートが一定以上 ②RSSIが一定以上（※5GHz帯と異なる） 5GHz帯へ帰属中のステアリング対象の無線クライアントの場合、 5GHz帯から2.4GHz帯へのバンド遷移は、 以下①②両方の条件を満たすこと ①無線クライアントへの送信レートが一定以上 ②RSSIが一定以下（※2.4GHz帯と異なる）
		帰属中の無線クライアントのRSSIが一定値以下であること	移動先バンドの通信負荷が、一定以下であること

本装置において、バンドステアリングを有効にした場合、
初期設定状態では、それぞれの機能は、以下の動作となります。

Pre-association steering 機能

新規無線クライアントに対し、5GHz 帯へ帰属先誘導を行います。

Idle post-association steering 機能

すでに帰属している無線クライアントに対し帰属先遷移がしにくい設定になっています。

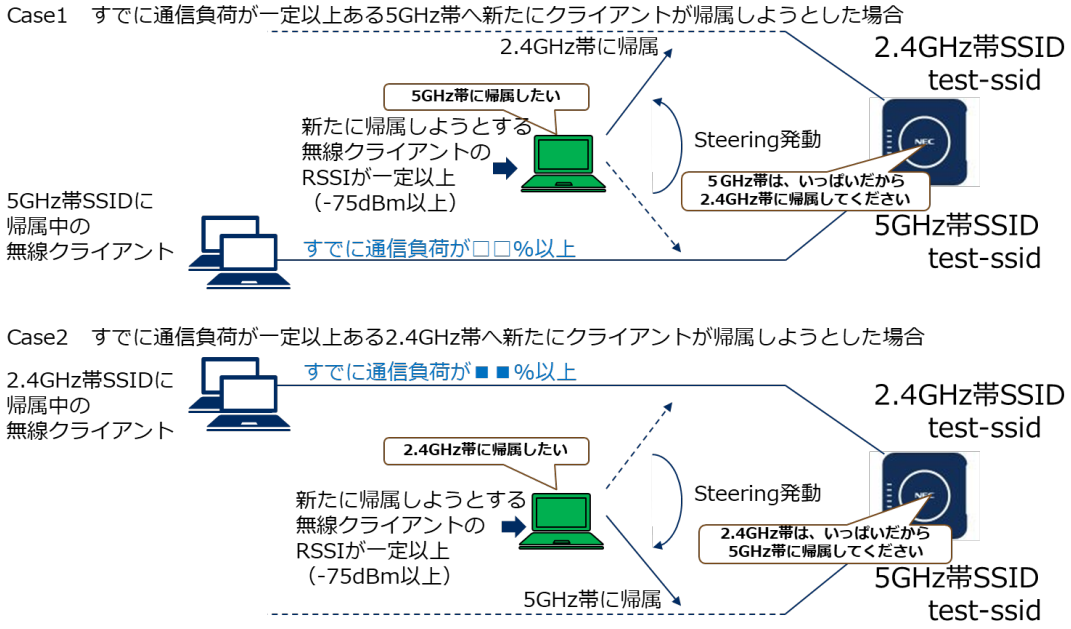
Active post-association steering 機能

すでに帰属している無線クライアントに対し帰属先遷移がしにくい設定になっています。

4.13.1. Pre-association steering 機能

新たに帰属しようとする無線クライアントを過負荷になっていないバンドに誘導帰属します。
すでに帰属している各バンドの通信負荷量は、1 分間継続している必要があります。

動作例



※遷移先バンドがmax-associations数に達している場合は、max-associations数に達していないバンドに帰属します。
※両バンドともすでに通信負荷が一定以上（Overload）あった場合、PCのドライバ優先設定に依存します。

動作例の設定

帰属先が設定以上の通信負荷がすでにあり、RSSI（-75dBm）値を満足する場合、他のバンドに帰属させます。

通信負荷の閾値を次ページにて設定が可能です。

radio0（5GHz 帯）の通信負荷閾値を設定する場合

AP(config)# interface radio0

AP(config-if-radio0)# load-balance pre-association-overload-thresh □□

AP(config-if-radio0)# !

AP(config)# write memory

radio1（2.4GHz 帯）の通信負荷閾値を設定する場合

AP(config)# interface radio1

AP(config-if-radio1)# load-balance pre-association-overload-thresh ■■

AP(config-if-radio1)# !

AP(config)# write memory

バンドステアリング機能を有効にする場合

AP(config)# ssid test-ssid

AP(config-ssid test-ssid)# load-balance enable

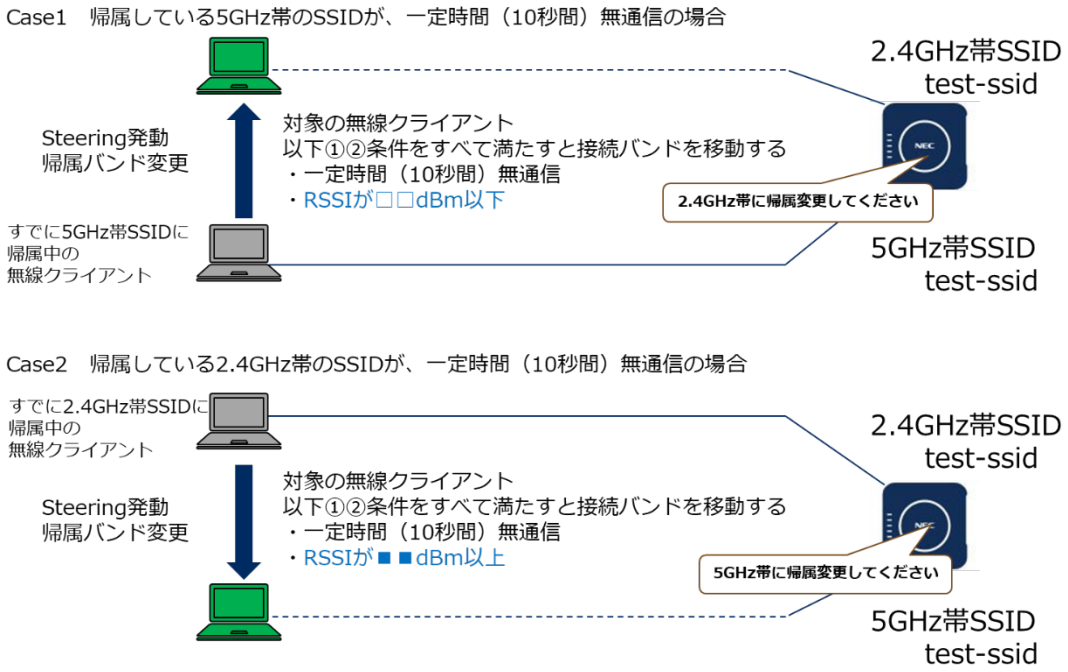
AP(config-ssid test-ssid)# !

AP(config)# write memory

4.13.2. Idle post-association steering 機能

すでに帰属している無線クライアントが IEEE802.11v をサポートしている場合、アップリンクデータ（keep alive 相当）を監視しています。
アップリンクデータ通信を行っていない無線クライアントに対しバンドステアリングします。

動作例



動作例の設定

次ページにて RSSI 閾値の設定が可能です。

radio0（5GHz 帯）に帰属している無線クライアントにおいて
無通信かつ RSSI が設定値以下の場合
※radio1（2.4GHz 帯）に遷移します。
AP(config)# interface radio0
AP(config-if-radio0)# load-balance idle-post-association-rssi-thresh □□
AP(config-if-radio0)# !
AP(config)# write memory

radio1（2.4GHz 帯）に帰属している無線クライアントにおいて
無通信かつ RSSI が設定した値以上の場合
※radio0（5GHz 帯）に遷移します。
AP(config)# interface radio1
AP(config-if-radio1)# load-balance idle-post-association-rssi-thresh ■■
AP(config-if-radio1)# !
AP(config)# write memory

バンドステアリング機能を有効にする場合
AP(config)# ssid test-ssid
AP(config-ssid test-ssid)# load-balance enable
AP(config-ssid test-ssid)# !
AP(config)# write memory

4.13.3. Active post-association steering 機能

すでに帰属している無線クライアントが IEEE802.11k と IEEE802.11v をサポートしている場合、データ通信中、

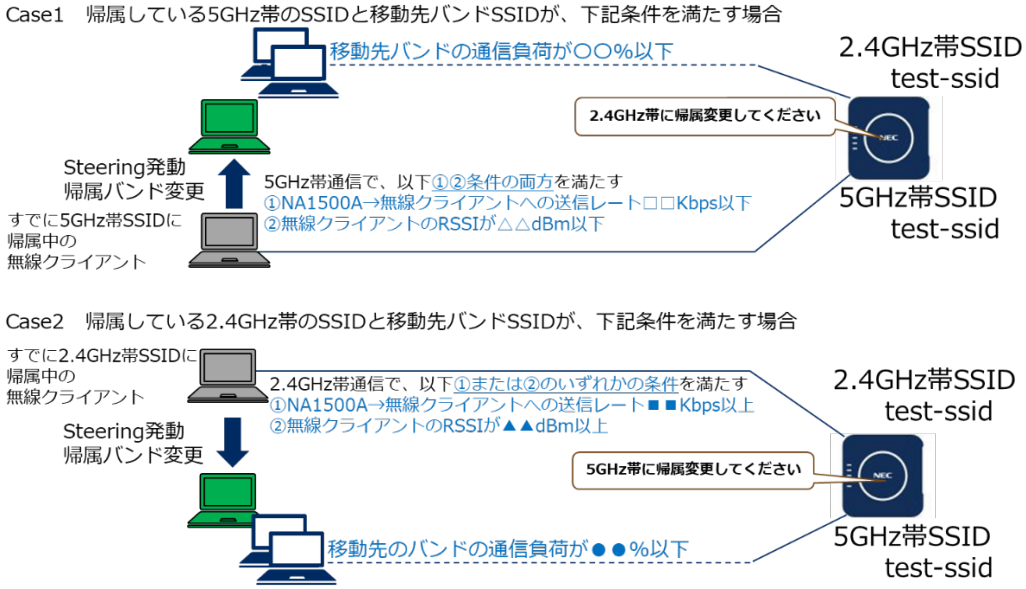
・無線クライアントへの送信レート

・RSSI 値

・移動先バンドの通信負荷

により指定したバンドへステアリングします。

動作例



動作例の設定

次ページにて以下の設定変更が可能です。

・無線クライアントへの送信レート

・RSSI 値

・移動先バンドの通信負荷

radio0（5GHz 帯）に帰属している無線クライアントにおいて
RSSI が設定値以下で、かつ、送信レートが設定値以下で、
遷移先バンド（2.4GHz 帯）の通信負荷が設定値以下の場合
※radio1（2.4GHz 帯）に遷移します。
AP(config)# interface radio0
AP(config-if-radio0)# load-balance active-post-association-rssi-thresh △△
AP(config-if-radio0)# load-balance active-post-association-txrate-thresh □□
AP(config-if-radio0)# load-balance active-post-association-mu-safety-thresh ○○
AP(config-if-radio0)# !
AP(config)# write memory

radio1（2.4GHz 帯）に帰属している無線クライアントにおいて
RSSI が設定した値以上で、または、送信レートが設定値以上で、
遷移先バンド（5GHz 帯）の通信負荷が設定値以下の場合
※radio0（5GHz 帯）に遷移します。
AP(config)# interface radio1
AP(config-if-radio1)# load-balance active-post-association-rssi-thresh ▲▲
AP(config-if-radio1)# load-balance active-post-association-txrate-thresh ■■
AP(config-if-radio1)# load-balance active-post-association-mu-safety-thresh ●●
AP(config-if-radio1)# !
AP(config)# write memory

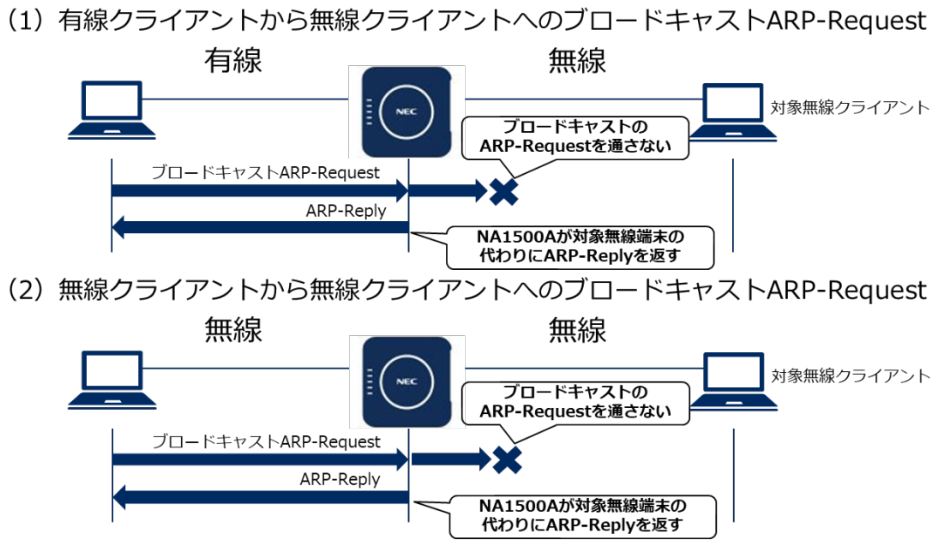
バンドステアリング機能を有効にする場合
AP(config)# ssid test-ssid
AP(config-ssid test-ssid)# load-balance enable
AP(config-ssid test-ssid)# !
AP(config)# write memory

4.14.　設定事例 14　ProxyARP の設定

4.14.1. ProxyARP 機能が有効（ip-proxy-arp enable [MODE]）の場合

4.14.1.1.　対象の無線クライアントが帰属している場合

ProxyARP 機能を有効（ip-proxy-arp enable [MODE=省略/1/2]）にすると、
ブロードキャスト ARP-Request を NA1500A が無線側に出さないように遮断し、
対象の無線クライアントが帰属していれば、対象の無線クライアントの ARP-Reply を
NA1500A が代わりに返します。



4.14.1.2.　対象の無線クライアントが帰属していない場合

対象の無線クライアントが帰属していない場合、設定モードにより動作が異なります。

(1)ProxyARP 機能がモード 1 の場合

（ip-proxy-arp enable [モード省略]　または、ip-proxy-arp enable 1　に設定）

対象の無線クライアントが帰属していない場合、ブロードキャスト ARP-Request を
NA1500A は、無線側へ遮断せずに転送します。

(2)ProxyARP 機能がモード 2 の場合

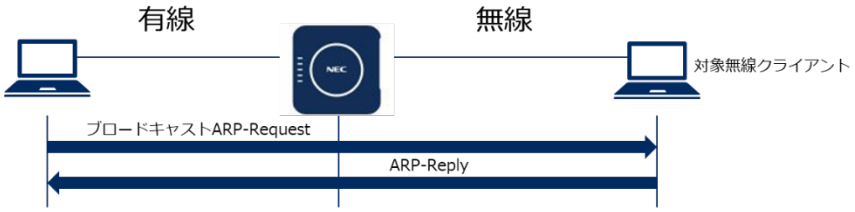
（ip-proxy-arp enable 2　に設定）

対象の無線クライアントが帰属していない場合、ブロードキャスト ARP-Request を
NA1500A は、無線側に出さないように遮断します。

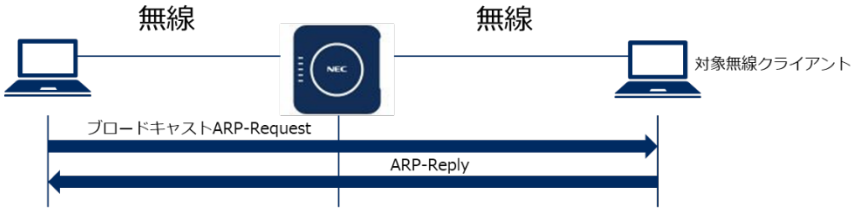
4.14.2. ProxyARP 機能が無効(no ip-proxy-arp enable)の場合

ProxyARP 機能が無効(no ip-proxy-arp enable)の場合、以下のとおり、
対象の無線クライアントが ARP-Reply を返します。

(1) 有線クライアントから無線クライアントへのブロードキャストARP-Request



(2) 無線クライアントから無線クライアントへのブロードキャストARP-Request



第5章　　利用シーンごとの設定例

利用シーンごとの各種機能の設定について説明します。

5.1. 公共エリアでの設定利用例

公共エリア（駅、空港、ホテル、学校など）での無線 LAN スポット（災害用無線 LAN 含む）では、不特定多数のユーザによる利用が考えられます。
公共エリアでの利用では、各無線クライアントのアクセス先および無線クライアント間に関する通信許可や遮断の設定などを検討し、設定する必要があります。

ケースに合わせて、次の内容を検討して、NA1500A へ設定するようにしてください。

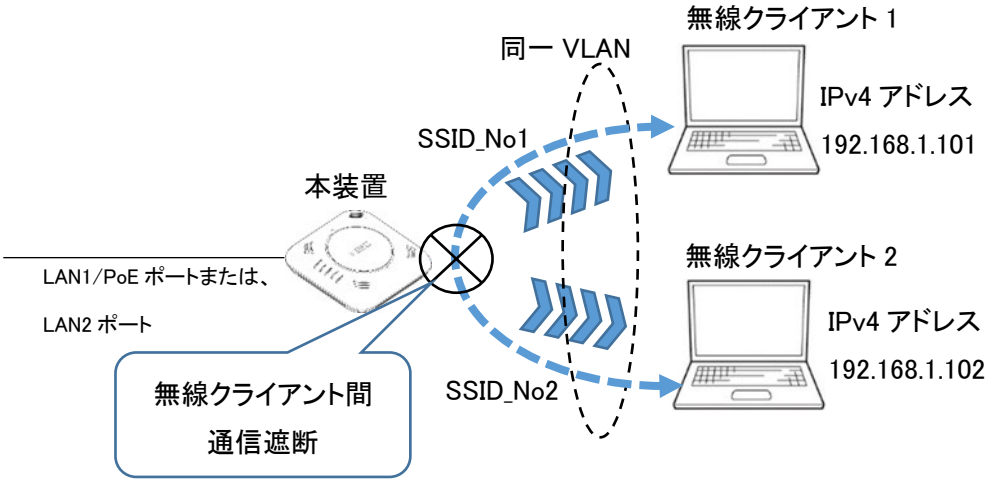
- ■ VLAN 内の異なる SSID へ帰属した無線クライアント間通信遮断
- ■ 同一 SSID へ帰属した無線クライアント間通信遮断
- ■ 複数の NA1500A を使用した場合の無線クライアント間通信遮断

次ページより、設定例を記載します。
※利用環境、使用ネットワーク構成によりカスタマイズが必要です。

5.1.1. VLAN 内の異なる SSID へ帰属した無線クライアント間通信遮断

VLAN 内の異なる SSID へ帰属した無線クライアント間通信遮断を行う場合は、
無線インタフェースの SSID 間分離機能の設定を行います。

以下は、同一 VLAN に属する SSID_No1 および SSID_No2 があり、
それぞれに帰属した端末（無線クライアント 1、無線クライアント 2）がある構成例です。
※設定は、利用環境や使用ネットワーク構成によりカスタマイズが必要です。



本構成における設定例は、以下のとおりです。
※本設定は、使用する無線インタフェースごとに設定します。

radio0（5GHz 帯）のみを使用する場合

```
AP(config)# interface radio0
AP(config-if radio0)# separate-ssid enable
AP(config-if radio0)# !
AP(config)# write memory
```

radio1（2.4GHz 帯）のみを使用する場合

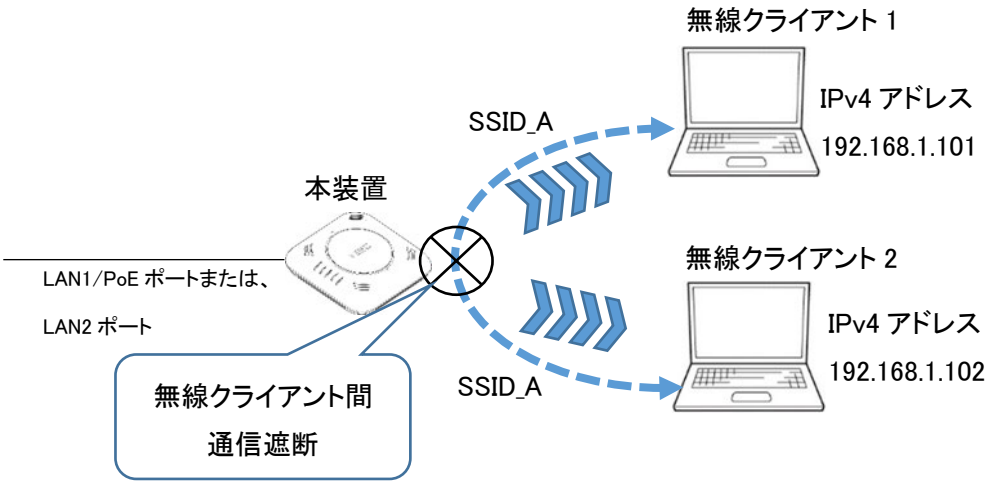
```
AP(config)# interface radio1
AP(config-if radio1)# separate-ssid enable
AP(config-if radio1)# !
AP(config)# write memory
```

radio0（5GHz 帯）および radio1（2.4GHz 帯）を使用する場合は、
上記 radio0（5GHz 帯）と radio1（2.4GHz 帯）に設定します。

5.1.2. 同一 SSID へ帰属した無線クライアント間通信遮断

同一 SSID へ帰属した無線クライアント間通信遮断を行う場合は、
SSID 内分離機能の設定を行います。

以下は、同一 SSID（SSID_A）に帰属した端末（無線クライアント 1、無線クライアント 2）がある構成例です。
※設定は、利用環境や使用ネットワーク構成によりカスタマイズが必要です。



本構成における設定例は、以下のとおりです。
※本設定は、対象の SSID ごとに設定します。

```
AP(config)# ssid SSID_A
AP(config-ssid SSID_A)# ssid-isolation enable
AP(config-ssid SSID_A)# !
AP(config)# write memory
```

5.1.3. 複数の NA1500A を使用した場合の無線クライアント間通信遮断

複数の NA1500A に収容された無線クライアント間の通信遮断を行う場合は、
IPv4 パケットアクセスリストの登録および、フィルタの設定を行います。

設定例は、
「4.9.4. 無線クライアントからルータを経由した通信のみを許可する」
を参照してください。
本設定は、対象の VLAN に属するすべての SSID に設定します。
※設定は、利用環境や使用ネットワーク構成によりカスタマイズが必要です。

第6章　　付録

商標、ライセンス、コピーライト

- NEC ロゴは、日本およびその他の国における日本電気株式会社の商標および登録商標です。
- NetMeister は、NECプラットフォームズ株式会社の登録商標です。
- UNIVERGE は、日本電気株式会社の登録商標です。
- Wi-Fi Alliance、WPA および WPA2 は、Wi-Fi Alliance の商標または登録商標です。
- その他、各会社名、各製品名およびサービス名などは各社の商標または登録商標です。

IEEE802.11ac 対応無線 LAN アクセスポイント

NA1500A

設定事例集

NWA-A06495-010-00

第 9.0 版　2024 年 08 月